

Гайдлайны андроид по выкладке в Google Play				
<p>Launch checklist Контрольный список запуска приложения</p> <p>Важно: с августа 2021 г. новые приложения должны публиковаться с Android App Bundle на Google Play. Новые приложения размером более 150 МБ теперь поддерживаются либо Play Feature Delivery или Play Asset Delivery.</p>	Developer Program Policies	Запрещенный контент	Нарушение прав ребенка	<p>Категорически запрещается публиковать приложения, в которых несовершеннолетние изображены в сексуальном контексте, в том числе приложения, пропагандирующие педофилию или недопустимые действия в отношении несовершеннолетних (например, ласки или ощупывание).</p> <p>Также запрещены приложения, предназначенные для детей, но содержащие материалы для взрослых, в том числе те приложения, которые содержат сцены насилия, изображения крови и увечий, а также демонстрируют или поощряют опасные или вредные действия. Запрещены приложения, формирующие негативное восприятие себя и собственного тела, например те, которые изображают в развлекательных целях пластическую хирургию, потерю веса и другие косметические коррективы внешнего вида.</p> <p>Если мы обнаружим материалы, содержащие изображение несовершеннолетних в сексуальном контексте, то сообщим об этом в соответствующие правоохранительные органы и удалим аккаунты всех пользователей, участвовавших в их распространении.</p>
			Неприемлемый контент	<p>1. Контент сексуального характера и непристойная лексика</p> <p>2. Дискриминационные высказывания</p> <p>3. Насилие</p> <p>4. Материалы террористического характера</p> <p>5. Трагические события</p> <p>6. Издевательства и угрозы</p> <p>7. Опасные товары (запрещается публиковать приложения, с помощью которых можно приобрести взрывчатые вещества, огнестрельное оружие, патроны, а также некоторые детали для огнестрельного оружия.)</p> <p>8. Марихуана</p> <p>9. Табачные изделия и алкоголь (запрещено публиковать приложения, с помощью которых можно приобрести табак (в том числе электронные сигареты и устройства для вейпинга), а также приложения, поощряющие незаконное или недопустимое потребление алкоголя и табака.)</p>
			Финансовые услуги	<p>Запрещено публиковать приложения, предоставляющие пользователям доступ к вводящим в заблуждение или вредоносным финансовым продуктам и услугам.</p> <p>Финансовыми считаются все продукты и услуги, связанные с управлением финансами, инвестициями и криптовалютами, в том числе персональные консультации.</p> <p>Если ваше приложение предлагает или рекламирует финансовые продукты и услуги, оно должно соответствовать требованиям государственного и муниципального законодательства во всех странах и регионах, для которых оно предназначено, – например, содержать информацию, особо оговоренную в местных законах.</p> <p>1. Бинарные опционы (запрещено публиковать приложения, позволяющие пользователям торговать бинарными опционами.)</p> <p>2. Криптовалюты (запрещено публиковать приложения, предназначенные для майнинга криптовалют на устройствах. Приложения, регулирующие майнинг криптовалют дистанционно, разрешены.)</p> <p>3. Потребительские кредиты</p> <p>Согласно нашим правилам, к потребительским кредитам относятся ссуды, одновременно предоставляемые физическим лицом или организацией отдельному клиенту не для приобретения основных средств или оплаты образования. Вместе с рекламой таких услуг необходимо опубликовать сведения о качестве, характеристиках, комиссии, графиках погашения, рисках и преимуществах кредитных предложений, чтобы пользователи могли принять взвешенное решение.</p> <p>Примеры: потребительские кредиты, кредиты наличными, займы между физическими лицами, кредиты под залог автомобиля.</p> <p>Не относятся к этой категории: ипотека, кредиты на образование и покупку автомобилей, возобновляемые кредиты (карты, персональные кредитные счета).</p> <p>Если вы предлагаете потребительские кредиты, в том числе напрямую, осуществляете поиск потенциальных клиентов или помогаете потребителям связаться со сторонними кредиторами, в метаданных приложения необходимо указывать следующую информацию:</p> <p>минимальный и максимальный период погашения долга;</p> <p>максимальная годовая процентная ставка, в которую обычно включается кредитная ставка, а также комиссии и прочие расходы за год, или же другая похожая ставка, соответствующая действующему законодательству;</p> <p>пример расчета общей стоимости займа, включая действующие комиссии;</p> <p>политика конфиденциальности, в которой подробно описано, как приложения получают доступ к информации пользователя, какие данные собираются и передаются, а также то, как они используются.</p> <p>Запрещено публиковать приложения, предлагающие потребительские кредиты, которые необходимо полностью погасить в течение 60 дней после выдачи кредита или быстрее (краткосрочные потребительские кредиты).</p> <p>4. Потребительские кредиты с высокой годовой процентной ставкой</p> <p>В США запрещены приложения, предлагающие потребительские кредиты с годовой процентной ставкой от 36 %. Публикуемые в США приложения, предлагающие потребительские кредиты, должны содержать информацию о максимальной годовой процентной ставке, рассчитанной в соответствии с законом "О справедливом кредитовании" (TILA).</p> <p>Эти правила относятся к приложениям, которые предлагают кредиты напрямую, осуществляют поиск потенциальных клиентов или помогают потребителям связаться со сторонними кредиторами.</p>

			<p>Приложения для азартных игр</p> <p>Допускаются приложения, которые позволяют или помогают участвовать в азартных онлайн-играх в странах, указанных в таблице ниже, если соблюдены все ограничения и правила Google Play, а разработчик подал заявку на распространение в Google Play приложений для азартных игр и получил разрешение. При этом разработчик является одобренным государственным оператором и/или зарегистрирован в местном ведомстве, отвечающем за игорную деятельность, и предоставил действующую лицензию для осуществления в стране той игровой деятельности, которую он предлагает.</p> <p>Мы допускаем только те лицензированные или разрешенные приложения, которые предлагают следующие виды азартных онлайн-игр (в таблице ниже показано, какие виды азартных игр разрешены в конкретных странах):</p> <ul style="list-style-type: none"> онлайн-казино; ставки на результаты спортивных соревнований; скачки (где регулирование и лицензирование осуществляются отдельно от ставок на спорт); лотереи; короткие фэнтези-турниры. <p>Разрешенные приложения должны соответствовать следующим требованиям:</p> <p>Разработчик подал заявку и получил разрешение на распространение приложения через Google Play.</p> <p>Приложение не нарушает действующие законы и отраслевые стандарты страны, в которой оно будет распространяться.</p> <p>У разработчика есть действующая лицензия на ведение игровой деятельности для всех стран или штатов/территорий, где распространяется приложение.</p> <p>Разработчик не предлагает те виды азартных игр, которые выходят за рамки его лицензии.</p> <p>Приложение недоступно для несовершеннолетних.</p> <p>Приложение недоступно в странах, штатах/регионах или географических районах, на которые не распространяется лицензия разработчика.</p> <p>Приложение распространяется в Google Play бесплатно и НЕ использует функцию оплаты контента через Google Play.</p> <p>Приложение можно бесплатно скачать из Google Play.</p> <p>Приложению присвоено возрастное ограничение "Только для взрослых" или эквивалентное согласно рейтингу IARC.</p> <p>В приложении и на его странице в Google Play есть описание принципов ответственной игры.</p>
			<p>Прочие приложения, связанные с азартными играми на реальные деньги, конкурсами и турнирами</p> <p>Во всех других приложениях, которые не соответствуют вышеперечисленным требованиям к приложениям для азартных игр, запрещается публиковать контент или сервисы, которые позволяют или помогают заключать пари, делать ставки или иным образом использовать реальные деньги (в том числе совершать покупки в приложении) с целью получить приз, который имеет реальную денежную стоимость. Это касается в том числе онлайн-казино, спортивных тотализаторов, лотерей и игр, в которых принимаются деньги, а выигрышем являются денежные и другие ценные призы (кроме программ, соответствующих описанным ниже требованиям к программам лояльности в игровой форме).</p> <p>Примеры нарушений</p> <p>Игры, в которых принимаются деньги в обмен на возможность выиграть денежных или иной материальный приз.</p> <p>Приложения, которые содержат элементы навигации или функции (пункты меню, вкладки, кнопки, компоненты WebView и т. д.) с призывом сделать ставку, заключить пари или принять участие в играх, конкурсах или соревнованиях с реальными денежными призами, например "Сделайте ставку!", "Зарегистрируйтесь!" или "Победите в соревновании!".</p> <p>Приложения, которые принимают ставки, используют внутреннюю валюту, выплачивают выигрыши или берут залог в обмен на возможность выиграть денежный или иной материальный приз.</p>
			<p>Программы лояльности в игровой форме</p> <p>Программы лояльности, которые поощряют пользователей материальными или денежными призами, разрешены, если они допускаются законом и не требуют получения дополнительной лицензии для азартных игр. Программы лояльности должны соответствовать перечисленным ниже требованиям Google Play.</p> <p>Все приложения (игровые и неигровые)</p> <p>Преимущества, бонусы или вознаграждения, предоставляемые в рамках программы лояльности, должны быть явно дополнительными и второстепенными по отношению к любой квалифицированной денежной транзакции в приложении (где квалифицированная денежная транзакция – отдельная транзакция с целью предоставления товаров или услуг; не связанных с программой лояльности). Преимущества, бонусы или вознаграждения не могут быть предметом покупки или иметь отношение к какому-либо способу обмена. В противном случае это будет считаться нарушением Правил в отношении азартных игр, игр и соревнований с реальными денежными призами.</p> <p>Например, ни одна часть квалифицированной денежной транзакции не может служить платой или ставкой для участия в программе лояльности. Также квалифицированная денежная транзакция не должна приводить к покупке товаров или услуг по повышенной цене.</p> <p>Игровые приложения</p> <p>Бонусные баллы или вознаграждения с бонусами, преимуществами и наградами, связанными с квалифицированной денежной транзакцией, могут начисляться и использоваться только на основе фиксированной пропорции при условии, что она четко обозначена в приложении и общедоступных официальных правилах программы. Преимущества или выкупная стоимость не могут быть получены, начислены или приумножены в зависимости от успеха пользователя в игре или случайного результата.</p> <p>Неигровые приложения</p> <p>Бонусные баллы или вознаграждения могут начисляться по результатам конкурса или случайного результата, если они соответствуют требованиям, указанным ниже. Для программ лояльности с преимуществами, бонусами или наградами, связанными с квалифицированной денежной транзакцией, необходимо:</p> <ul style="list-style-type: none"> разместить в приложении официальные правила программы; если система вознаграждения меняется или основана на случайном или вероятностном выборе, в рамках официальных правил программы необходимо раскрыть: 1) вероятность – для любой системы вознаграждения, в которой для определения победителя используются фиксированные коэффициенты; 2) метод выбора (например, переменные, используемые для определения победителя) – для других подобных программ; указать в официальных правилах программы с розыгрышами, потерями или другими подобными промоакциями фиксированное число победителей, срок подачи заявок и дату вручения призов для каждой такой промоакции; указать фиксированные коэффициенты начисления и погашения бонусных баллов или наград на видном месте в приложении, а также в официальных правилах программы.
			<p>Приложения, распространяемые в Google Play, которые содержат рекламу азартных игр, а также игр, конкурсов и турниров на реальные деньги</p> <p>Приложения с рекламой азартных игр, а также игр, конкурсов и соревнований с реальными денежными призами разрешены, если выполняются перечисленные ниже условия.</p> <p>Приложение и объявление не нарушают законы и отраслевые стандарты страны, в которой будет показываться объявление. Это же условие относится и к рекламодателю.</p> <p>Объявление соответствует всем действующим местным требованиям к лицензированию продуктов и услуг, связанных с азартными играми.</p> <p>Приложение не показывает рекламу азартных игр лицам, не достигшим 18 лет.</p> <p>Приложение не входит в программу "Приложения для всей семьи".</p> <p>Лица, не достигшие 18 лет, не входят в целевую аудиторию приложения.</p> <p>Если рекламируются приложения для азартных игр (см. выше), на целевой странице объявления, в описании приложения в Google Play или в самом приложении должны содержаться четкие сведения о принципах ответственной игры.</p> <p>Приложение не является симулятором азартных игр (таких как казино или виртуальные игровые автоматы).</p> <p>Приложение не оказывает услуги, связанные с азартными играми, а также играми, потерями и соревнованиями с реальными денежными призами или сопутствующими функциями (например, не помогает делать ставки, выводить выигрыши, отслеживать счет, котировки и результаты или управлять игровыми фондами).</p> <p>Приложение не продвигает азартные игры на реальные деньги и связанные с ними сервисы.</p> <p>Реклама азартных игр, а также игр, потерей и соревнований с реальными денежными призами допускается только в приложениях, соответствующих всем перечисленным требованиям, и в разрешенных приложениях для азартных игр (см. выше) или коротких фэнтези-турниров (см. ниже) при условии, что они соответствуют требованиям 1–6.</p>

				<p>Приложения для коротких фэнтези-турниров</p> <p>Приложения для коротких фэнтези-турниров, соответствующие требованиям действующего местного законодательства, разрешены, если выполняются перечисленные ниже условия.</p> <p>Приложение или 1) распространяется исключительно в США; или 2) соответствует требованиям к приложениям для азартных игр. Для распространения приложения за пределами США разработчик должен подать заявку, как указано выше.</p> <p>Разработчик подал заявку и получил разрешение на распространение приложения в Google Play.</p> <p>Приложение не нарушает законы и отраслевые стандарты стран, в которых оно распространяется.</p> <p>Возможность делать ставки или проводить денежные транзакции в приложении недоступна для несовершеннолетних.</p> <p>Приложение распространяется в Google Play бесплатно и НЕ использует функцию оплаты контента через Google Play.</p> <p>Приложение можно бесплатно скачать из Google Play.</p> <p>Приложению присвоено возрастное ограничение "Только для взрослых" или эквивалентное согласно рейтингу IARC.</p> <p>В приложении и на его странице в Google Play есть описание принципов ответственной игры.</p> <p>Приложение не нарушает действующие законы и отраслевые стандарты тех штатов или территорий США, где оно будет распространяться.</p> <p>У разработчика есть действующая лицензия на распространение приложения для каждого штата или территории США, где такая лицензия требуется.</p> <p>Если у разработчика нет лицензии на распространение приложения в каких-то штатах или на некоторых территориях США, то оно должно быть там недоступно.</p> <p>Приложение недоступно в тех штатах и на тех территориях США, где приложения для коротких фэнтези-турниров запрещены законом.</p>
			Незаконные действия	<p>Запрещено публиковать приложения, которые способствуют совершению незаконных действий или поощряют их.</p> <p>Вот примеры наиболее распространенных нарушений:</p> <p>Реклама и продажа без рецепта препаратов, продаваемых только по рецепту, или запрещенных наркотических веществ.</p> <p>Изображение того, как несовершеннолетние используют или приобретают наркотики, алкоголь и табачные изделия, а также поощрение этого.</p> <p>Инструкции по производству запрещенных наркотических веществ, в том числе по выращиванию наркотических растений.</p>
			Контент, созданный пользователями	<p>К этой категории относится контент, создаваемый пользователями, который виден или доступен нескольким пользователям приложения.</p> <p>Приложения, которые содержат создаваемый пользователями контент, должны соответствовать перечисленным ниже требованиям.</p> <p>Перед созданием контента и загрузкой пользовательских материалов в приложении необходимо принять условия или правила использования этого приложения.</p> <p>Вы должны дать определение неприемлемого контента и поведения, а также объяснить, что такие материалы запрещены. Эта информация должна соответствовать правилам программы для разработчиков и присутствовать в условиях или правилах использования приложения.</p> <p>Создаваемый пользовательский контент оперативно и регулярно модерруется настолько, насколько это уместно для данного типа материалов.</p> <p>Если пользовательский контент транслируется, то неприемлемые материалы должны удаляться из приложения как можно скорее.</p> <p>При модерации пользовательского контента в приложениях с дополненной реальностью (включая систему отчетов в приложении) необходимо обращать внимание как на сам неприемлемый пользовательский контент в дополненной реальности (например, на изображения сексуального характера), так и на место, к которому он привязан (иногда контент дополненной реальности привязан к территории с ограниченным доступом, например военной базе или объекту частной собственности, и может вызвать проблемы для собственника).</p> <p>В приложении можно без труда сообщать о неприемлемом пользовательском контенте и удалять его.</p> <p>Разработчик удаляет или блокирует аккаунты пользователей, оскорбляющих других людей и нарушающих условия или правила использования приложения.</p> <p>Разработчик принял меры предосторожности для того, чтобы монетизация в приложении не способствовала нежелательному поведению пользователей.</p> <p>Мы удаляем из Google Play приложения, предназначенные в основном для неприемлемых пользовательских материалов. Так же мы поступаем с приложениями, в которых размещают главным образом неподобающий контент или которые известны наличием таких материалов.</p>
			Запрещенные вещества	<p>В Google Play нельзя публиковать приложения для рекламирования или продажи запрещенных веществ, даже если они заявлены как законные. Примеры:</p> <p>Все продукты из неполного списка запрещенных лекарственных препаратов и пищевых добавок.</p> <p>Продукты, содержащие эфедру.</p> <p>Продукты, содержащие хорионический гонадотропин человека (ХГЧ) как средство для похудения или контроля за весом либо в сочетании с анаболическими стероидами.</p> <p>Диетические добавки и средства растительного происхождения, содержащие сильнодействующие или опасные ингредиенты.</p> <p>Продукты, в описании которых содержатся ложные заявления о пользе для здоровья, например средства, якобы сравнимые по эффективности с отпускаемыми по рецепту лекарствами или иными подконтрольными препаратами.</p> <p>Продукты, не прошедшие государственную сертификацию, в рекламе которых подразумевается, что они безопасны или эффективны при лечении или профилактике заболеваний.</p> <p>Продукты, в отношении которых введены правительственные санкции либо приняты запретительные или предупредительные меры со стороны контролирующих органов.</p> <p>Продукты, наименования которых очень похожи на названия запрещенных пищевых добавок, фармацевтических или иных веществ с контролируемым оборотом и могут ввести в заблуждение.</p> <p>Подробную информацию о запрещенных фармацевтических препаратах и пищевых добавках можно найти на сайте www.legitscript.com.</p>
		Выдача себя за другое лицо		<p>Когда разработчик выдает себя за другое лицо, это вредит и клиентам, и всему сообществу разработчиков. Мы запрещаем публиковать приложения, которые вводят пользователя в заблуждение путем выдачи автора за другое лицо.</p> <p>Разработчик вводит пользователя в заблуждение относительно связи с другой компанией/разработчиком.</p> <p>Приложения, названия и значки которых похожи на названия и значки других продуктов или сервисов.</p> <p>Приложения, которые ложно представлены как официальные продукты другой компании.</p>
		Интеллектуальная собственность		<p>Когда недобросовестный разработчик копирует чужую работу или пытается ввести пользователей в заблуждение, это вредит и клиентам, и всему сообществу разработчиков. Призываем вас отказаться от плагиата в своих приложениях.</p>
			Незаконное использование контента, защищенного авторским правом	<p>Запрещается нарушать чужие авторские права. Изменение материалов, защищенных авторским правом, также может привести к нарушению. В некоторых случаях разработчики должны доказать свое право на использование того или иного авторского контента.</p> <p>Не рекомендуется использовать чужой контент для демонстрации возможностей своего приложения. Безопаснее всего создать оригинальные материалы.</p>
			Поощрение нарушения авторских прав	<p>Запрещено публиковать приложения, поощряющие нарушение авторских прав или способствующие этому. Если вы не уверены, что ваше приложение не нарушает это правило, обратитесь за советом к юристу.</p>

			Нарушение прав на товарный знак	<p>Запрещено публиковать приложения, нарушающие права на товарный знак. Товарным знаком называют слово, символ или их сочетание, указывающие на производителя товара или поставщика услуг. Он дает владельцу исключительные права на его использование применительно к данному товару или услуге.</p> <p>Нарушением данных прав считается ненадлежащее или несанкционированное использование идентичного либо очень похожего товарного знака с целью дать неверное представление об источнике продукта. Если в вашем приложении присутствуют товарные знаки других продуктов, которые могут ввести пользователей в заблуждение, оно может быть заблокировано.</p>
			Поддельные товары	<p>Запрещено публиковать приложения, в которых продаются или рекламируются поддельные товары. Речь идет об изделиях, на которых есть обозначения, идентичные чужим логотипам / товарным знакам или очень похожие на них. Это позволяет выдавать поддельный товар за подлинный.</p>
		Нарушение конфиденциальности, злоупотребление ресурсами устройства и мошенничество	Данные пользователя	<p>К данным пользователя относятся сведения, предоставленные им, а также полученные в ходе его работы, в том числе информация об устройстве. Обязательно сообщите, как и для чего вы будете использовать и собирать данные, а также получать и предоставлять к ним доступ. Применяя информацию в целях, о которых вы не заявили, запрещено. Если ваше приложение обрабатывает личные или конфиденциальные данные, оно должно соответствовать требованиям, перечисленным в разделе "Личная и конфиденциальная информация". Эти правила Google Play используются наряду с требованиями действующего законодательства о конфиденциальности и защите данных.</p>
				<p>Личная и конфиденциальная информация</p> <p>К личным и конфиденциальным пользовательским данным относятся, в том числе, сведения, позволяющие идентифицировать личность, финансовые, платежные, учетные и контактные данные (включая телефонную книгу, данные звонков и SMS), данные о местоположении устройства и списке других приложений на устройстве, данные микрофона и камеры, а также другая конфиденциальная информация об устройстве или его использовании. Если ваше приложение обрабатывает личные или конфиденциальные данные, оно должно соответствовать перечисленным ниже требованиям.</p> <p>Доступ к личным и конфиденциальным данным, полученным через приложение, а также их сбор, использование и передача допускаются только для предоставления или улучшения функций (например, для обеспечения возможностей, указанных на странице приложения в Google Play). Если вы планируете использовать эти данные также для показа рекламы, ваши приложения должны соответствовать Правилам размещения рекламы.</p> <p>Политика конфиденциальности должна быть приведена в соответствующем поле Play Console и в самом приложении. В политике конфиденциальности и в информации об использовании личных данных, размещенной в самом приложении, необходимо объяснить, как приложение получает доступ к данным пользователя, что это за данные, а также как они собираются, используются и передаются. Кроме того, в политике конфиденциальности нужно указать, кто и при каких обстоятельствах может получить доступ к личной и конфиденциальной информации. Обрабатывать все личные и конфиденциальные данные пользователя необходимо безопасным образом, в том числе с применением современных методов шифрования, например протокола HTTPS.</p> <p>Прежде чем использовать данные, доступ к которым регулируется разрешениями Android, приложение должно запросить динамическое разрешение (когда появится возможность). Не продавайте личную и конфиденциальную информацию.</p>
				<p>Раскрытие информации и разрешение на использование данных</p> <p>Если у пользователей нет разумных оснований ожидать, что их личные и конфиденциальные данные будут применяться для предоставления и улучшения функций приложения, соответствующих правилам (например, когда их данные собираются в фоновом режиме), необходимо соблюдать перечисленные ниже требования.</p> <p>В приложении должна содержаться информация о сборе, использовании и передаче личных данных, соответствующая следующим требованиям:</p> <p>Информация должна быть в самом приложении, а не только в его описании или на сайте. Информация должна отображаться при обычном использовании приложения, без вызова меню или настроек.</p> <p>В информации должно быть указано, какие данные использует или собирает приложение.</p> <p>В ней должно объясняться, как именно приложение использует и передает данные.</p> <p>Нельзя публиковать эту информацию только в политике конфиденциальности и условиях использования.</p> <p>Нельзя включать эту информацию в документы, которые не имеют отношения к сбору личных и конфиденциальных данных.</p> <p>Показав эту информацию пользователю, необходимо сразу запросить у него согласие и, когда появится возможность, динамическое разрешение. Использовать или собирать личную и конфиденциальную информацию без согласия ее владельца нельзя. Запрос составляется в соответствии со следующими правилами:</p> <p>Запрос нужно сформулировать предельно ясно и показать в диалоговом окне.</p> <p>Необходимо попросить пользователя подтвердить разрешение (например, нажать кнопку или установить флажок).</p> <p>Нельзя считать согласием ситуации, когда пользователь намеренно или случайно закрывает окно с запросом.</p> <p>Запрос не должен автоматически закрываться или исчезать до того, как пользователь его примет или отклонит.</p>
				<p>EU-U.S., Swiss Privacy Shield</p> <p>Если вы получаете доступ к личным данным пользователей, предоставленным компанией Google и созданным на территории Европейского союза или Швейцарии, если используете либо обрабатываете эту информацию и по ней можно прямо или косвенно установить личность человека, то вы должны:</p> <p>Соблюдать все действующие законы, директивы и правила в отношении конфиденциальности, безопасности и защиты личных данных.</p> <p>Получать доступ к личным данным и использовать их только в тех целях, с которыми согласился их владелец.</p> <p>Применять необходимые организационные и технические средства для защиты личных данных от потери, недопустимого использования, несанкционированного или незаконного доступа, разглашения, изменения и нарушения целостности.</p> <p>Обеспечивать личным данным необходимую защиту в соответствии с принципами соглашения Privacy Shield.</p> <p>Вы обязаны регулярно сверяться с этими требованиями. Если соблюдать их станет невозможно или возникнет серьезный риск того, что вы не сможете обеспечить соответствие им, немедленно сообщите нам об этом по адресу data-protection-office@google.com и прекратите обработку личных данных или как можно скорее восстановите их защиту.</p> <p>Начиная с 16 июля 2020 года компания Google больше не использует EU-U.S. Privacy Shield (соглашение о правилах передачи персональных данных между ЕС и США) при передаче персональных данных из Европейской экономической зоны или Великобритании в США. Подробнее... Узнать больше можно в разделе 9 Соглашения.</p>

			<p>Разрешения</p> <p>Пользователю должно быть понятно, для чего вам требуется разрешение. Запрашивать разрешения можно только в том случае, если они необходимы для работы функций и сервисов, которые уже есть в приложении и описаны на его странице в Google Play. Нельзя использовать разрешения, предоставляющие доступ к данным пользователя или устройства, для не заявленных, не внедренных или запрещенных функций или целей. Ни при каких обстоятельствах нельзя продавать личные или конфиденциальные данные, полученные с разрешения пользователя.</p> <p>Запрашивайте доступ к данным в контексте (позатпно). Это поможет пользователям понять, для чего вам нужно то или иное разрешение. Используйте данные только в тех целях, на которые пользователь дал согласие. Если в дальнейшем вам понадобится использовать их в других целях, вам необходимо будет получить явное согласие пользователя на это.</p> <p>Ограниченные разрешения</p> <p>Кроме того, к разрешениям, которые указаны ниже или обозначены в документации для разработчиков как опасные, специальные или требующие определенной подписи, применяются дополнительные требования и ограничения:</p> <p>Конфиденциальные данные пользователя или устройства, полученные в рамках таких разрешений, можно передавать третьим лицам только в том случае, если это нужно для работы или улучшения уже внедренных функций и сервисов приложения, в котором эти данные получены. Также передача данных возможна, если этого требует действующее законодательство или сделка по слиянию, поглощению компании или продаже активов. Вы должны уведомить об этом пользователя юридически приемлемым способом. Во всех остальных случаях продажа и передача данных пользователя запрещена.</p> <p>Если пользователь отклоняет запрос на ограниченное разрешение, вы не должны пытаться переубедить его. Нельзя заставлять пользователей предоставлять разрешения, которые не являются критически важными. В этом случае вы обязаны приложить обоснованные усилия для того, чтобы все равно обеспечить пользователю доступ к функциям приложения (например, предусмотреть возможность ввода телефонного номера вручную, если доступ к списку вызовов запрещен).</p> <p>Категорически запрещено использовать разрешения, нарушающие официальные рекомендации для разработчиков Android по работе с разрешениями для приложений или существующие правила (в том числе в отношении повышения привилегий).</p> <p>В отношении некоторых ограниченных разрешений могут действовать дополнительные требования, описанные ниже. Соблюдение этих условий помогает обеспечивать конфиденциальность пользователей. В очень редких случаях мы можем сделать исключение, если приложение выполняет какие-либо важные и востребованные функции, которые в настоящий момент не могут быть реализованы другим способом. Принимая решение в таких ситуациях, мы учитываем потенциальные угрозы конфиденциальности и безопасности данных.</p>
			<p>Разрешения на доступ к SMS и списку вызовов</p> <p>SMS и список вызовов считаются личными и конфиденциальными данными. К ним применяются положения раздела Личная и конфиденциальная информация, а также следующие ограничения:</p> <p>Группа разрешений на доступ к списку вызовов (например, READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS) - приложение должно быть зарегистрировано как помощник или обработчик звонков по умолчанию.</p> <p>Группа разрешений на доступ к SMS (например, READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS) - приложение должно быть зарегистрировано как помощник или обработчик SMS по умолчанию.</p> <p>Приложениям, которые не могут быть назначены помощником или обработчиком SMS или звонков по умолчанию, запрещено запрашивать подобные разрешения. В том числе нельзя указывать соответствующие теги в манифесте. Запрашивать такие разрешения можно только после того, как пользователь сам установит приложение в качестве помощника или обработчика для SMS или звонков по умолчанию. Как только пользователь изменит свой выбор, приложение должно прекратить использовать эти разрешения. Допустимые сценарии использования и исключения описаны в этой статье Справочного центра.</p> <p>Приложения могут использовать указанные выше разрешения и полученные благодаря им данные только для работы основных функций (например, для обеспечения возможностей, явно указанных в описании приложения). Основными называются функции, без которых приложение невозможно использовать. Передача данных, в том числе для использования по лицензии, а также предоставление доступа к ним допускается только в целях, необходимых для работы основных функций приложения или сервисов в нем. Запрещено использовать данные в любых других целях, включая улучшение сервисов или приложений, рекламу и маркетинг. Нельзя использовать альтернативные способы (включая другие разрешения, API и сторонние источники) для получения данных, связанных с разрешениями на доступ к списку вызовов и SMS.</p>
			<p>Разрешения на доступ к данным о местоположении</p> <p>Данные о местоположении устройства считаются личными и конфиденциальными. К ним применяются положения раздела Личная и конфиденциальная информация, а также следующие требования:</p> <p>Приложения не должны использовать сведения, защищенные разрешениями на доступ к данным о местоположении (например, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION), если эти сведения не нужны для работы функций и сервисов, которые уже есть в приложении.</p> <p>Ни при каких обстоятельствах нельзя запрашивать доступ к данным о местоположении, если они будут использоваться только для рекламы и аналитики. Приложения, в которых эти данные будут использоваться в том числе для показа рекламы (после получения разрешения от пользователя), должны соответствовать правилам размещения рекламы.</p> <p>Запрашивать следует минимально необходимый уровень доступа (то есть доступ к приблизительным, а не к точным данным о местоположении и разрешение на использование в активном режиме, а не в фоновом). Важно, чтобы доступ действительно требовался для работы сервиса или функции, имеющихся в приложении, и пользователи должны ясно понимать, почему для той или иной функции нужен запрашиваемый уровень доступа. Мы можем отказать в публикации приложений, которые запрашивают фоновый доступ к данным о местоположении без веского обоснования.</p> <p>Данные о местоположении можно использовать только в том случае, если они нужны для работы функций, которые полезны для пользователя и связаны с основным назначением приложения.</p> <p>Приложение может получать доступ к сведениям о местоположении в активном режиме (например, когда с приложением работают), если использование этих данных:</p> <p>необходимо для выполнения в приложении действия, инициированного пользователем; прекращается сразу после выполнения этого действия.</p> <p>Приложения, разработанные специально для детей, должны соответствовать требованиям программы Приложения для всей семьи.</p>
			<p>Разрешение на доступ ко всем файлам</p> <p>Информация о файлах и папках на устройстве пользователя считается личной и конфиденциальной информацией и должна соответствовать положениям раздела Личная и конфиденциальная информация, а также следующим требованиям:</p> <p>Приложения должны запрашивать доступ к хранилищу устройства только в том случае, если это необходимо для работы приложения. Они не могут запрашивать доступ к хранилищу от имени третьего лица для любых целей, не связанных с ключевыми функциями приложения.</p> <p>Устройствам Android с версией R или более поздней для управления доступом к общему хранилищу необходимо разрешение MANAGE_EXTERNAL_STORAGE. Все приложения, предназначенные для этой версии системы и запрашивающие доступ к общему хранилищу ("Доступ ко всем файлам"), проходят соответствующую проверку перед публикацией. Приложения, которые могут использовать это разрешение, должны явно предлагать пользователям включить доступ ко всем файлам в меню настроек "Специальный доступ для приложений".</p>

				<p>Разрешение на доступ к списку пакетов (приложений)</p> <p>Список установленных приложений на устройстве пользователя считается личной и конфиденциальной информацией, которая должна соответствовать положениям раздела Личная и конфиденциальная информация, а также следующим требованиям:</p> <p>Приложения, основной функцией которых является запуск, поиск других приложений на устройстве или взаимодействие с ними, могут получить соответствующее разрешение на просмотр других установленных приложений следующим образом:</p> <p>Широкий доступ к списку пакетов. Это возможность приложения видеть все установленные на устройстве приложения (пакеты). Приложения, предназначенные для ОС с API уровня 30 и выше, могут получить широкий доступ к списку приложений с помощью разрешения QUERY_ALL_PACKAGES лишь в некоторых случаях, а именно когда для корректной работы приложению необходимо получать данные о других приложениях и/или взаимодействовать с ними.</p> <p>Нельзя использовать разрешение QUERY_ALL_PACKAGES, если приложение может работать с более ограниченным набором приложений. Например, вы можете выбрать отдельные пакеты, доступ к которым будет запрашивать ваше приложение.</p> <p>Существуют альтернативные методы, которые позволяют получить практически такой же уровень доступа, как с помощью разрешения QUERY_ALL_PACKAGES. Использовать их допускается только для работы ключевых функций приложения (важных для пользователя) и только для взаимодействия с приложениями, которые были найдены этими альтернативными методами.</p> <p>Чтобы узнать, в каких случаях допускается использование разрешения QUERY_ALL_PACKAGES, ознакомьтесь с этой статьей Справочного центра.</p> <p>Ограниченный доступ. Приложение с ограниченным доступом будет запрашивать только информацию об определенных пакетах, используя более узкие методы, например с помощью указанных параметров в файле манифеста. Этот метод можно использовать, когда приложение соответствует правилам и ему требуется доступ к управлению другими приложениями или взаимодействию с ними.</p> <p>Доступ к списку пакетов должен быть напрямую связан с основным назначением приложения или его основными функциями (то есть с функциями, ради которых пользователь работает с приложением).</p> <p>Ни при каких обстоятельствах нельзя продавать данные о списке приложений, установленных из Google Play, а также предоставлять к ним доступ для аналитики и получения дохода от рекламных объявлений.</p>
			Злоупотребление ресурсами устройства и сети	<p>Запрещается публиковать приложения, которые нарушают работу устройства пользователя, других устройств, компьютеров, серверов, сетей, API или сервисов (включая другие приложения на устройстве, сервисы Google и сети операторов связи), а также вмешиваются в их работу, получают несанкционированный доступ к ним или вредят иным образом.</p> <p>Приложения, размещаемые в Google Play, должны соответствовать требованиям оптимизации для Android, зафиксированным в Основных критериях качества приложений.</p> <p>Приложения, которые распространяются в Google Play, не должны изменять свой код каким-либо способом, кроме обновления через Google Play. Они также не должны скачивать исполняемый код (например, файлы в формате DEX, JAR или SO), созданный сторонними разработчиками. Это правило не распространяется на код, который запускается на виртуальной машине и имеет ограниченный доступ к API Android (например, код JavaScript в компоненте WebView или браузерере).</p> <p>Запрещено использовать код, который создает или использует уязвимости безопасности. Информация о самых актуальных проблемах безопасности содержится в нашей Программе повышения безопасности приложений для разработчиков.</p>
			Введение в заблуждение	<p>Мы запрещаем публиковать приложения, которые пытаются ввести пользователей в заблуждение или способствуют недобросовестной деятельности, включая приложения, заявленные функции которых невозможно реализовать на устройстве. Информация о приложении, его описание, а также фото и видео должны соответствовать его функциональности. Приложения не должны имитировать функции или предупреждения операционной системы и других программ. Любые изменения настроек устройства должны производиться с ведома и согласия пользователя. Кроме того, у пользователя должна быть возможность отменить изменения.</p> <p>Заявления, вводящие в заблуждение</p> <p>Скриншоты, значки, названия, описания и другие материалы приложения не должны содержать ложную или вводящую в заблуждение информацию.</p> <p>Несанкционированные изменения настроек устройства</p> <p>Запрещается публиковать приложения, которые вносят изменения в настройки устройства или другие приложения без ведома и согласия пользователя. К настройкам устройства относятся параметры системы и браузера, закладки, ярлыки, значки и виджеты приложений на главном экране.</p> <p>Кроме того, запрещено указанное ниже.</p> <p>Приложения, которые изменяют настройки или функции устройства с согласия пользователя, но таким образом, что это нельзя легко отменить.</p> <p>Приложения и содержащиеся в них объявления, которые каким-либо образом добавляют на устройство рекламу или ссылки на сервисы третьих сторон.</p> <p>Приложения, которые обманым путем побуждают пользователя удалять или деактивировать программы других разработчиков либо изменять настройки устройства.</p> <p>Приложения, которые призывают пользователей удалять или отключать программы других разработчиков либо изменять настройки устройства. Исключение составляют приложения, обеспечивающие безопасность устройства или данных.</p>
				<p>Пособничество недобросовестной деятельности</p> <p>Запрещается публиковать приложения, которые рассчитаны на использование в недобросовестных целях. Например, приложения для создания паспортов и других удостоверений личности, номеров социального страхования, дипломов, кредитных карт и водительских прав. Информация о приложении, его название, описание, а также изображения и видеоролики должны соответствовать его функциональности и содержанию, а само приложение должно работать так, как этого ожидает пользователь.</p> <p>Дополнительные ресурсы приложения (например, игровые объекты) могут быть доступны для скачивания, только если они необходимы для использования приложения. При этом они должны соответствовать всем правилам Google Play, а приложение должно сообщить пользователю размер этих файлов до того, как начать скачивание.</p> <p>Заявления о том, что приложение создано для розыгрыша или с другими несерьезными намерениями, не избавляет разработчиков от ответственности и необходимости соблюдать наши правила.</p>
				<p>Манипулирование медиаконтентом</p> <p>Запрещается публиковать приложения, которые способствуют распространению или позволяют создавать ложную или вводящую в заблуждение информацию или заявления в форме изображений, видео и/или текста. Мы не разрешаем публиковать приложения, предназначенные для распространения или сохранения изображений, видео и/или текстов, которые демонстративно вводят пользователей в заблуждение и могут причинять ущерб в связи с важными событиями, политической сферой, социальными вопросами и другими общественно значимыми темами.</p> <p>Приложения, которые манипулируют медиаконтентом или изменяют его, выходя за общепринятые рамки допустимых корректировок для повышения четкости и качества при подготовке к публикации, должны явным образом сообщать об этом в измененном контенте или добавлять к нему водяные знаки, если обычному пользователю может быть неочевидно, что материалы были изменены. Исключения могут быть сделаны для тем, представляющих общественный интерес, а также очевидных примеров сатиры или пародии.</p>

			Искажение фактов	<p>Мы запрещаем приложения и аккаунты разработчиков, которые:</p> <p>выдают себя за других лиц или другие организации, а также скрывают или искажают свою основную цель или сведения о владельцах;</p> <p>намеренно вводят пользователей в заблуждение, например скрывают или искажают информацию о стране происхождения или предоставляют контент пользователям в других странах;</p> <p>сотрудничают с другими приложениями, сайтами, разработчиками и аккаунтами в целях сокрытия или фальсификации данных о приложении или разработчике, а также другой важной информации (это относится к контенту, который имеет политическую, социальную или общественную направленность).</p>
		Монетизация и реклама	Платежи	<p>1. Разработчики, которые взимают средства за скачивание приложений в Google Play, должны использовать платежную систему Google Play.</p> <p>2. Приложения, распространяемые в Google Play, должны использовать платежную систему Google Play, если они требуют или принимают оплату за доступ к функциям или сервисам, включая любые функции приложения, цифровой контент или товары.</p> <p>Примерами функций или сервисов приложений, требующих использования платежной системы Google Play, являются в том числе следующие покупки в приложении:</p> <ul style="list-style-type: none"> Предметы (например, виртуальная валюта, дополнительные жизни, дополнительное время игры, новые предметы, персонажи и аватары). Подписки (например, подписка на спортивный, игровой, образовательный, музыкальный, видео- и прочий контент). Функционал и контент (например, версия приложения без рекламы или функции, недоступные в бесплатной версии). Облачные программные продукты (например, хранилища данных, а также ПО для бизнеса и управления финансами). <p>Платежную систему Google Play нельзя использовать в перечисленных ниже случаях.</p> <p>Если речь идет преимущественно о следующих платежах:</p> <ul style="list-style-type: none"> Примечание. На некоторых рынках для продажи физических товаров или услуг можно использовать Google Pay. Подробная информация приведена на странице Google Pay для разработчиков. покупка или аренда товаров (например, продуктов питания, одежды, товаров для дома и электронных устройств); услуга, оказываемая в реальном мире (например, транспорт, услуги клининга, авиабилет, абонемент в тренажерный зал, доставка еды, билеты на концерт); оплата счета по кредитной карте или счета за коммунальные услуги (например, кабельное телевидение и телекоммуникационные услуги). При переводах средств другим пользователям, в том числе пожертвований и оплаты покупок на онлайн-аукционах. Если вы оплачиваете контент или сервис, связанный с азартными онлайн-играми, как описано в разделе Приложения для азартных игр правил Азартные игры на реальные деньги, игры и соревнования. Для платежей, связанных с категорией товаров, которая считается неприемлемой в соответствии с правилами Платежного центра относительно контента. <p>3. Приложения, не упомянутые в части 2 раздела 2, не должны предлагать пользователям способы оплаты, отличные от платежной системы Google Play. В частности, запрещено упоминать другие способы оплаты в следующих источниках:</p> <ul style="list-style-type: none"> на странице приложения в Google Play; в объявлениях внутри приложения, предлагающих покупку контента; в компонентах WebView, кнопках, ссылках, объявлениях, сообщениях и других призывах к действию внутри приложения; в пользовательском интерфейсе, в том числе при регистрации и создании аккаунта, нельзя перенаправлять пользователя к способу оплаты, отличному от платежной системы Google Play. <p>4. Виртуальная валюта должна использоваться только в том продукте, в котором она была куплена.</p> <p>5. Разработчики обязаны явно и четко информировать пользователей об условиях и ценах на приложение или любые функции и подписки. Цены внутри приложения должны совпадать с ценами, которые появляются в платежном интерфейсе Google Play. Если за доступ к функциям, указанным в описании приложения в Google Play, взимается плата, вы обязаны предупредить об этом пользователей в описании.</p> <p>6. Если при покупках в приложении или игре можно получить случайные виртуальные предметы, как, например, в лутбоксе, вы должны четко сообщить пользователю непосредственно перед покупкой, какова вероятность получения таких предметов.</p>
			Реклама	<p>Запрещено публиковать приложения, в которых есть объявления, вводящие в заблуждение или прерывающие работу приложения. Объявления должны появляться только внутри приложения, быть приемлемыми для его целевой аудитории, а также соответствовать всем нашим правилам.</p> <p>Использование данных о местоположении в целях рекламы</p> <p>Приложения, которые используют доступ к данным о местоположении устройства для показа рекламы, должны соответствовать положениям раздела Личная и конфиденциальная информация, а также следующим требованиям:</p> <ul style="list-style-type: none"> Нужно ясно донести до пользователя, что если он предоставит разрешение, то данные о местоположении его устройства будут собираться или использоваться для показа рекламы. Вы должны сообщить об этом в обязательной политике конфиденциальности приложения, а также добавить ссылки на политики конфиденциальности рекламных сетей в отношении использования данных о местоположении. Разрешения на доступ к данным о местоположении могут запрашиваться только для работы функций и сервисов, которые есть в приложении. Нельзя запрашивать доступ к данным о местоположении, если он будет использоваться только для рекламы.
				<p>Объявления, вводящие в заблуждение</p> <p>Рекламные объявления не должны копировать интерфейс какого-либо приложения, системного уведомления или предупреждения. Пользователю должно быть понятно, к какому приложению относятся те или иные объявления.</p>
				<p>Монетизация функций блокировки экрана</p> <p>Запрещено показывать рекламу и размещать платные функции на заблокированном экране, кроме тех случаев, когда приложение предназначено исключительно для управления заблокированным экраном.</p>
				<p>Объявления, прерывающие работу приложения</p> <p>К этой категории относятся объявления, которые появляются в неожиданных местах, могут приводить к непреднамеренным нажатиям и нарушать функциональность устройства.</p> <p>Запрещается вынуждать пользователя нажимать на объявление или отправлять личные данные для получения полного доступа к приложению. Межстраничные объявления могут отображаться только внутри приложения. Если в приложении есть межстраничные или другие объявления, которые прерывают обычный процесс использования, они должны легко закрываться.</p>
				<p>Взаимодействие с приложениями, рекламой других разработчиков и функциями устройства</p> <p>Объявления в вашем приложении не должны влиять на приложение других разработчиков и рекламу в них, а также на работу устройства, его портов и системных или физических кнопок. В частности, это относится к плавающим объявлениям, сопутствующим функциям и рекламным блокам-виджетам. Объявления должны появляться только внутри приложения.</p>
				<p>Неприемлемые объявления</p> <p>Не только сам контент приложения должен соответствовать нашим правилам. Объявления в приложении должны быть приемлемы для его целевой аудитории.</p>

				<p>Использование рекламного идентификатора Android</p> <p>В сервисах Google Play 4.0 появились новые API, а также идентификатор для рекламодателей и тех, кто предоставляет услуги аналитики. Условия использования идентификатора приведены ниже.</p> <p>Использование. Рекламный идентификатор Android должен использоваться только для размещения рекламы и анализа ее показателей. При каждом обращении к идентификатору должны проверяться значения параметров "Отключить подбор рекламы" и "Отключить персонализацию рекламы".</p> <p>Связь с информацией, позволяющей идентифицировать личность, и другими идентификаторами.</p> <p>Рекламный идентификатор нельзя связывать с постоянными идентификаторами устройства, такими как SSAID, MAC-адрес или IMEI-код, в рекламных целях. Рекламный идентификатор можно связывать с данными, позволяющими идентифицировать личность, только при условии явно выраженного согласия пользователя.</p> <p>Использование в аналитических целях. Рекламный идентификатор нельзя связывать с данными, позволяющими идентифицировать личность, или постоянными идентификаторами устройства, такими как SSAID, MAC-адрес или IMEI-код, без явно выраженного согласия пользователя.</p> <p>Уважение предпочтений пользователя. Новый идентификатор, присвоенный после сброса, нельзя связывать с предыдущим или его данными без явно выраженного согласия пользователя. Кроме того, нужно учитывать предпочтения пользователя в отношении подбора и персонализации рекламы. Если эти функции отключены, то вам запрещается использовать рекламный идентификатор для создания пользовательского профиля в рекламных целях или для показа персонализированных объявлений. К разрешенным приемам относятся контекстная реклама, ограничение частоты показов, отслеживание конверсий, сообщения о нарушениях и обнаружение угроз безопасности и случаев мошенничества.</p> <p>Уведомление пользователей. В примечании о конфиденциальности, соответствующем требованиям законодательства, пользователю необходимо сообщить о сборе и использовании рекламных идентификаторов, а также о настоящих правилах. Подробная информация о наших стандартах конфиденциальности приведена в разделе Данные пользователя.</p> <p>Соблюдение условий использования. Рекламный идентификатор можно применять только в соответствии с настоящими правилами, причем это условие распространяется на всех, кому вы можете предоставить идентификатор в ходе коммерческой деятельности. Во всех приложениях, загружаемых или публикуемых в Google Play, следует использовать рекламный идентификатор (если он доступен на устройстве). Применять для рекламных целей другие идентификаторы устройств запрещено.</p>
			Подписки	<p>Разработчикам запрещается вводить пользователей в заблуждение относительно подписок или контента, который предлагается в приложениях. Ваше предложение должно быть сформулировано четко и ясно. Это относится к его размещению как на заставках, так и в самом приложении.</p> <p>В приложении необходимо четко изложить свое предложение. Среди прочего необходимо ясно указать условия предложения, стоимость подписки и периодичность платежного цикла, а также уточнить, необходима ли подписка для работы с приложением. При этом все сведения должны быть указаны полностью, чтобы для ознакомления с информацией пользователю не требовалось выполнять дополнительные действия.</p>
				<p>Бесплатные пробные версии и предложения для новых пользователей</p> <p>Еще до того, как пользователь приобретет подписку, вы должны ясно и точно сообщить ему условия предложения, включая его продолжительность и цену, а также описание доступного контента или сервисов. Не забудьте указать, как и когда пользователь перейдет с бесплатной пробной версии на платную подписку, уточнить стоимость платной подписки, а также сообщить, что подписку можно отменить до окончания бесплатного пробного периода.</p>
				<p>Управление подписками и их отмена</p> <p>Разработчик обязан явно сообщить пользователю информацию о том, как изменить или отменить подписку в приложении.</p> <p>Согласно правилам Google Play при отмене купленной в приложении подписки возврат средств за текущий расчетный период не производится. Однако контент, доступный по подписке, предоставляется пользователю до конца этого периода. Затем подписка отменяется.</p> <p>В качестве поставщика контента или доступа вы можете установить более гибкие правила возврата платежей. Убедитесь, что правила подписки, ее отмены и возврата платежей не противоречат действующему законодательству, а также обязательно сообщайте пользователям обо всех изменениях в этих правилах.</p>
			Программа рекламы в приложениях для всей семьи	<p>Как описано в правилах программы "Приложения для всей семьи", при размещении рекламы в приложении, предназначенном только для детей, необходимо использовать рекламные SDK, которые прошли самостоятельную сертификацию и подтвердили соответствие правилам Google Play, включая приведенные ниже требования к сертификации рекламных SDK. Если приложение разработано как на детей, так и на взрослых, вы должны предусмотреть проверку возраста пользователя и убедиться, что дети будут видеть только те объявления, для которых использовались рекламные SDK с самостоятельной сертификацией. В приложениях, участвующих в программе "Приложения для всей семьи", запрещается использовать другие рекламные SDK.</p> <p>Использование сертифицированных рекламных SDK становится обязательным только в том случае, если вы в целом применяете SDK для показа рекламы детям. Вы несете ответственность за содержание объявлений и сбор сведений согласно правилам в отношении пользовательских данных и правилам программы "Приложения для всей семьи". При соблюдении этих условий мы не требуем сертификацию:</p> <p>для показа собственной рекламы, когда SDK используется для мерчандайзинга и перекрестного продвижения ваших приложений или другого вашего медиаконтента;</p> <p>для прямых сделок с рекламодателями, при которых SDK используется только для управления ресурсами.</p>
	Данные для Google Play и продвижение		Продвижение приложения	<p>Запрещено публиковать приложения, прямо или косвенно связанные с методами продвижения, которые вводят в заблуждение или иным образом причиняют вред пользователям, а также сообществу разработчиков. Считается, что методы вводят в заблуждение и причиняют вред, если они нарушают Правила программы для разработчиков.</p> <p>Примеры распространенных нарушений:</p> <p>Использование рекламы, вводящей в заблуждение, на сайтах, в приложениях и других ресурсах. Например, к ней относятся объявления, похожие на системные уведомления.</p> <p>Использование рекламы сексуального характера для перенаправления пользователей на страницу приложения в Google Play.</p> <p>Продвижение и установка, в результате которых происходит перенаправление пользователей в Google Play или скачивание приложения без предварительного запроса.</p> <p>Нежелательная реклама через SMS.</p> <p>Вы обязаны следить за тем, чтобы эти правила соблюдались в рекламных сетях, партнерских программах и объявлениях, связанных с вашим приложением.</p>
			Метаданные	<p>Мы запрещаем публиковать приложения с ложными, неправильно отформатированными, недостаточными, нерелевантными, излишними или неудобными метаданными. К метаданным, помимо всего прочего, относятся название и описание приложения, его значок, скриншоты и рекламные изображения, а также название компании-разработчика. Описание приложения должно быть понятным и грамотным. Мы также запрещаем включать в описание отзывы пользователей без указания автора цитаты.</p>
			Оценки, отзывы и количество установок	<p>Разработчикам запрещено предпринимать попытки изменить позицию какого-либо приложения в рейтинге Google Play, например с помощью мошеннических установок, оплаченных или ложных оценок и отзывов.</p>
			Возрастные ограничения	<p>Система возрастных ограничений в Google Play создана для того, чтобы разработчики могли сообщать пользователям, для какой аудитории подходят приложения в их стране. Она включает официальные категории Международной коалиции возрастной классификации (IARC). Представительства IARC в отдельных странах при определении возрастной категории контента в приложении следуют соответствующим рекомендациям. Запрещена публикация приложений без указаний возрастных ограничений.</p> <p>Для чего нужны возрастные ограничения</p> <p>Возрастные ограничения помогают клиентам (особенно родителям) понять, есть ли в приложении потенциально нежелательный для них контент. Они позволяют блокировать или фильтровать контент для отдельных пользователей, а также определенных стран и регионов в соответствии с законодательством. С помощью возрастных ограничений можно оценить, есть ли у приложения право участвовать в специальных программах для разработчиков.</p>

				<p>Как присваиваются возрастные ограничения</p> <p>Чтобы получить возрастное ограничение, необходимо заполнить анкету в Play Console. В ней нужно подробно описать весь контент в приложении. На основе ваших ответов несколько уполномоченных организаций присвоят приложению определенное возрастное ограничение. Искажение фактов о контенте может привести к удалению или блокировке приложения, поэтому важно предоставить как можно более точную информацию.</p> <p>Заполнить анкету нужно для каждого приложения независимо от даты публикации, иначе ему будет присвоен статус "Без классификации". Такие приложения удаляются из Google Play.</p> <p>Если вы вносите в контент или функции приложения изменения, которые влияют на ответы в анкете, вы должны заполнить ее в Play Console ещё раз.</p> <p>Как оспорить возрастное ограничение</p> <p>Если вы не согласны с присвоенным ограничением, подайте апелляцию напрямую в IARC. Для этого перейдите по ссылке в сертификате, полученном по электронной почте.</p>
				<p>Любые новостные приложения (далее – Новостные приложения) в Play Console должны соответствовать всем описанным ниже требованиям.</p> <p>Новостные приложения, требующие оформления подписки, перед покупкой должны предоставлять часть контента в режиме предварительного просмотра.</p> <p>Новостные приложения ДОЛЖНЫ:</p> <ul style="list-style-type: none"> содержать информацию об издатель новостей и их источниках, включая, помимо прочего, данные о владельце, ссылку на официальный сайт, где опубликованы новости, достоверную и поддающуюся проверке контактную информацию и сведения об оригинальном издателе каждой статьи; иметь специальный сайт (или страницу в приложении) с контактной информацией. Эту страницу должно быть легко найти (например, нажав на ссылку в нижней части главной страницы или на панели навигации сайта), и она должна содержать актуальную контактную информацию издателя новостей, включая как минимум контактный адрес электронной почты и номер телефона. <p>Обратите внимание, что ссылки на аккаунты в социальных сетях не считаются достаточной контактной информацией. Кроме того, приложения, которые содержат в основном контент, созданный пользователями (например, приложения социальных сетей), не считаются Новостными приложениями.</p> <p>Новостные приложения НЕ ДОЛЖНЫ:</p> <ul style="list-style-type: none"> содержать материалы с явными грамматическими и орфографическими ошибками; содержать только статический контент (например, материалы, которые не обновлялись несколько месяцев); иметь в качестве основной цели получение дохода от рекламы или партнерский маркетинг. <p>Обратите внимание, что Новостные приложения могут использовать рекламу и другие формы маркетинга для получения дохода, если основной целью приложения не является реализация продуктов и услуг или получение дохода от рекламы.</p> <p>Новостные агрегаторы должны явно указывать источник контента, причем каждый источник должен соответствовать правилам в отношении новостей.</p>
		Спам и функциональность	Спам	<p>Запрещено публиковать скопированные и низкосортные приложения, а также приложения, распространяющие спам.</p>
				<p>Спам в сообщениях</p> <p>Запрещено публиковать приложения, которые отправляют от имени пользователя SMS, письма и другие виды сообщений, не давая пользователю возможности проверить содержание и получателя.</p>
				<p>Спам с целью перенаправления трафика</p> <p>Запрещено публиковать приложения, основной целью которых является привлечение трафика на веб-сайт без разрешения владельца или администратора сайта.</p>
				<p>Повторяющийся контент</p> <p>Запрещено публиковать приложения, которые полностью повторяют другие приложения, уже размещенные в Google Play. Каждое приложение должно предоставлять уникальный контент или услугу.</p>
				<p>Рекламные приложения</p> <p>Запрещается публиковать приложения, основной целью которых является показ рекламы.</p>
			Функциональность	<p>Убедитесь, что ваше приложение работает стабильно и корректно, а также представляет ценность для пользователей.</p>
				<p>Неработающие приложения</p> <p>Запрещается публиковать приложения, которые дают сбой, принудительно закрываются, зависают или работают с другими ошибками.</p>
		Вредоносное ПО		<p>Правило простое: экосистема Android, включающая Google Play и устройства пользователей, не должна подвергаться воздействию вредоносного ПО. Руководствуясь этим принципом, мы стараемся делать экосистему Android безопасной для пользователей и их устройств на базе Android.</p> <p>Вредоносным ПО считается любой код, который может представлять угрозу для пользователя, а также его данных или устройств. Например, к вредоносному ПО относятся потенциально опасные приложения (ПОП), а также исполняемые файлы и модификации фреймворков, относящиеся к таким категориям, как троянские программы, фишинг и шпионское ПО. Мы постоянно обновляем этот список и добавляем новые категории.</p> <p>Вредоносные программы могут различаться по типу и принципу действия, но, как правило, преследуют какие-либо из следующих целей:</p> <ul style="list-style-type: none"> вмешательство в работу устройства пользователя; получение контроля над устройством пользователя; выполнение удаленных операций, позволяющих получать доступ к зараженному устройству или каким-либо образом использовать его; передача персональных или учетных данных с устройства без ведома и согласия пользователя; рассылка с зараженного устройства спама или команд, которые затрагивают другие устройства или сети; мошеннические действия по отношению к пользователю. <p>Приложения, исполняемые файлы и модификации фреймворков, даже если они изначально не были созданы с вредоносными целями, могут считаться потенциально опасными и представлять угрозу для пользователя. Дело в том, что они могут действовать по-разному в зависимости от целого ряда факторов. Компоненты, которые могут представлять риск для одних устройств Android, совершенно безвредны для других. Например, вредоносные программы, использующие устаревшие API, не станут угрозой для устройств, на которых установлена последняя версия ОС Android, в отличие от устройств с более ранними версиями. Приложения, исполняемые файлы и модификации фреймворков помечаются как вредоносные или потенциально опасные, если они представляют явную угрозу для некоторых или всех пользователей и устройств Android.</p>
				<p>Бэкдоры</p> <p>Код, который позволяет удаленно выполнять на устройстве нежелательные, потенциально опасные операции.</p> <p>Такие операции могут включать процессы, из-за автоматического выполнения которых приложение, исполняемый файл или модификация фреймворка попадет в другие категории вредоносного ПО. В целом бэкдор – это способ, с помощью которого потенциально опасные операции могут быть выполнены на устройстве. Поэтому бэкдор сложно поставить в один ряд с такими категориями, как мошенническое списание средств или коммерческое шпионское ПО. В результате Google Play Защита при определенных обстоятельствах может посчитать набор бэкдоров уязвимостью.</p>

			<p>Мошенническое списание средств</p> <p>Код, который приводит к автоматическому списанию средств пользователя обманным способом.</p> <p>Существует три категории мошеннических списаний средств через операторов мобильной связи: SMS-мошенничество, мошенничество со звонками и мошенничество с оформлением подписки или оплатой контента.</p> <p>SMS-мошенничество В этом случае код приводит к отправке платных SMS без согласия пользователя или скрывает соглашения, содержащие информацию о передаче SMS, или сообщения, в которых оператор связи уведомляет о списании средств или подтверждает оформление подписки.</p> <p>Бывает, что код не скрывает от пользователя отправку сообщений, но способствует SMS-мошенничеству другими путями. Примеры: сокрытие определенных разделов соглашения с информацией о передаче SMS или представление этих разделов в нечитаемом виде, блокировка сообщений, в которых оператор связи уведомляет пользователя о списании средств или подтверждает подписку.</p> <p>Мошенничество со звонками В этом случае код приводит к звонкам на платные номера без согласия пользователя.</p> <p>Мошенничество с оформлением подписки или оплатой контента В этом случае код используется для того, чтобы обманным путем заставить человека приобрести подписку или оплатить контент через оператора мобильной связи.</p> <p>К этой категории относятся все списания средств, кроме тех, которые вызваны платными SMS и платными звонками. Примеры: оплата через оператора связи, использование беспроводной точки доступа (WAP) и передача минут мобильной связи. Мошенничество с WAP особенно популярно. Оно может использоваться для того, чтобы обманом заставить человека нажать кнопку в незаметно загружающемся прозрачном компоненте WebView. В результате подписка оформляется, а SMS или письмо с подтверждением транзакции перехватывается, чтобы пользователь не узнал о списании средств.</p>
			<p>ПО для преследования</p> <p>Код, который собирает и/или передает личные или конфиденциальные пользовательские данные с устройства без согласия или уведомления пользователя, а также не показывает уведомление, когда происходит отправка такой информации.</p> <p>Приложения для преследования, которые отслеживают личные и конфиденциальные данные пользователей, передают такие данные или предоставляют третьим лицам доступ к ним.</p> <p>Единственными приемлемыми приложениями для наблюдения являются приложения, предназначенные для родительского или корпоративного контроля. При этом должны полностью соблюдаться приведенные ниже требования. С помощью этих приложений запрещается следить за другими лицами (например, за супругом или супругой) даже с ведома и согласия таких лиц и при условии показа уведомления о передаче информации.</p> <p>Опубликованные в Google Play приложения, не предназначенные для преследования, но отслеживающие действия пользователя на устройстве, должны соответствовать как минимум перечисленным ниже требованиям.</p> <p>В описании приложения не должно говориться, что это шпионское ПО или решение для секретной слежки.</p> <p>Приложения не должны скрывать свои функции отслеживания или вводить пользователя в заблуждение по этому поводу.</p> <p>Во время работы таких приложений должны постоянно отображаться уведомление о том, что приложение запущено, и уникальный значок, позволяющий четко идентифицировать приложение.</p> <p>В приложениях и на их страницах в Google Play не должно быть способов активировать функции, нарушающие эти правила, или получить доступ к таким функциям. Например, запрещены ссылки на не соответствующие требованиям APK-файлы, размещенные не в Google Play.</p> <p>Вы несете полную ответственность за соответствие вашего приложения законам страны, где оно будет распространяться. Приложения, нарушающие законы стран, для распространения в которых они опубликованы, подлежат удалению.</p>
			<p>Атака типа "отказ в обслуживании" (DoS)</p> <p>Код, который незаметно для пользователя запускает атаку типа "отказ в обслуживании" (DoS) или принимает участие в распределенной атаке такого типа, направленной на другие системы и ресурсы.</p> <p>Пример: отправка большого количества HTTP-запросов для создания чрезмерной нагрузки на удаленные серверы.</p>
			<p>Загрузчики вредоносного ПО</p> <p>Код, который сам по себе безвреден, но скачивает другие потенциально опасные приложения.</p> <p>Код может быть загрузчиком вредоносного ПО, если выполняется хотя бы одно из условий:</p> <p>есть основания считать, что он создан для распространения потенциально опасных приложений, скачивает такие приложения или содержит код, который может скачивать и устанавливать приложения;</p> <p>как минимум 5 % приложений, скачанных этим кодом, являются потенциально опасными (то есть при минимальном пороге в 500 скачанных приложений должно быть обнаружено хотя бы 25 потенциально опасных).</p> <p>Ведущие браузеры и приложения для обмена файлами не считаются загрузчиками вредоносного ПО, если:</p> <p>скачивание в них не запускается без участия пользователя;</p> <p>скачивание потенциально опасных приложений начинается только после того, как пользователь дает на это согласие.</p>
			<p>Угроза для устройств не на базе Android</p> <p>Код, потенциально опасный для других платформ.</p> <p>Приложения с таким кодом безопасны для устройств Android и их пользователей, но содержат компоненты, которые могут нанести вред другим платформам.</p>
			<p>Фишинг</p> <p>Код, полученный якобы из надежного источника, который запрашивает учетные или платежные данные пользователя, а затем передает их третьим лицам. К этой же категории относится код, который перехватывает учетные данные при их передаче.</p> <p>Обычно фишингу подвергаются номера кредитных карт, а также учетные данные для аккаунтов в банковских системах, играх и социальных сетях.</p>

				<p>Повышение привилегий</p> <p>Код, который нарушает целостность системы, проникая в тестовую среду, получая более высокий уровень привилегий или изменяя или отключая доступ к основным функциям, связанным с безопасностью.</p> <p>Примеры:</p> <p>Приложения, которые нарушают модель разрешений Android или крадут учетные данные (такие как токены OAuth) из других приложений.</p> <p>Приложения, которые препятствуют удалению или остановке функций.</p> <p>Приложения, которые отключают модуль SELinux.</p> <p>Приложения, которые без разрешения пользователя получают root-доступ через повышение привилегий, относятся к категории "Получение root-доступа".</p>
				<p>Программы-вымогатели</p> <p>Код, который получает полный или частичный контроль над устройством или данными на нем и требует, чтобы для восстановления доступа пользователь заплатил деньги или выполнил какое-либо действие.</p> <p>Некоторые из таких программ шифруют данные на устройстве и требуют деньги за их расшифровку и/или получают полномочия администратора, что не позволяет пользователю удалить программу-вымогатель. Примеры:</p> <p>Программы, которые блокируют пользователю доступ к устройству и требуют деньги за его восстановление.</p> <p>Программы, которые шифруют данные и требуют плату якобы за их расшифровку.</p> <p>Программы, которые получают доступ к менеджеру правил устройства, из-за чего пользователь не может удалить эти программы.</p> <p>Код, распространяемый вместе с устройством, предназначенный в первую очередь для привилегированного управления устройством, может быть исключен из категории программ-вымогателей, если он соответствует требованиям к безопасности блокировки и управления, а также к раскрытию информации и получению согласия пользователей.</p>
				<p>Получение root-доступа</p> <p>Код, который получает root-доступ к устройству.</p> <p>Такой код не всегда является вредоносным. К примеру, некоторые приложения заранее предупреждают пользователя о том, что получат root-доступ к устройству, и не выполняют других опасных действий, характерных для потенциально опасных приложений.</p> <p>Вредоносные приложения не уведомляют пользователя о том, что они получают root-доступ к устройству, или уведомляют, но также выполняют другие действия, характерные для потенциально опасных приложений.</p>
				<p>Спам</p> <p>Код, который отправляет незапрашиваемые сообщения контактам пользователя или использует устройство в качестве ретранслятора писем со спамом.</p>
				<p>Шпионское ПО</p> <p>Код, который передает личные данные с устройства без уведомления и согласия пользователя.</p> <p>Например, признаком шпионского ПО считается передача без ведома пользователя следующей информации:</p> <ul style="list-style-type: none"> списка контактов; фотографий и других файлов с SD-карты, а также файлов, которые не принадлежат приложению; писем пользователя; списка вызовов; списка SMS; истории веб-поиска или закладок в используемом по умолчанию браузеру; информации из каталогов /data/ других приложений. <p>Шпионским также может считаться ПО, которое следит за пользователем, например записывает аудио и входящие звонки или крадет данные приложений.</p>
				<p>Троянские приложения</p> <p>Код, который кажется безвредным (например, обычной игрой), но выполняет нежелательные действия по отношению к пользователю.</p> <p>Эта классификация обычно используется в сочетании с другими категориями потенциально опасных приложений. Троянское приложение выглядит безвредно, но содержит скрытый вредоносный компонент. Например, игра, которая в фоновом режиме отправляет платные SMS с устройства без ведома пользователя.</p>
				<p>Примечание о необычных приложениях</p> <p>Google Play Защита может посчитать новые и редкие приложения необычными при отсутствии достаточного количества данных, указывающих на безопасность. Это не означает, что приложение является вредоносным. Но в число безопасных оно сможет попасть только после дополнительной проверки.</p>
				<p>Примечание к категории "Бэкдоры"</p> <p>Включение кода в категорию бэкдоров зависит от того, что именно он делает. Чтобы код считался бэкдором, он должен позволять запускать процессы, из-за автоматического выполнения которых код попадет в другую категорию вредоносного ПО. Например, если в приложении разрешена динамическая загрузка кода и динамически загружаемый код извлекает SMS, такое приложение будет считаться бэкдором.</p> <p>Но если в приложении разрешено выполнение произвольного кода и у нас нет оснований считать, что этот код добавлен для выполнения вредоносных процессов, такое приложение не будет отнесено к бэкдорам. Вместо этого мы отметим, что оно имеет уязвимость, и попросим разработчика устранить ее.</p>

		Нежелательное ПО для мобильных устройств	Mobile Unwanted Software	<p>В Правилах в отношении нежелательного ПО отмечено, что нежелательные программы в основном имеют следующие характеристики:</p> <p>Они не соответствуют описанию, чем вводят пользователей в заблуждение. Они устанавливаются обманным путем (самостоятельно или вместе с другими программами). Они не сообщают пользователю о своих важных функциях. Они вносят неожиданные изменения в систему. Они собирают или передают конфиденциальную информацию без ведома пользователя. Они собирают или передают конфиденциальную информацию небезопасным способом (например, не по протоколу HTTPS). Они устанавливаются в комплекте с другими программами без ведома пользователя.</p> <p>На мобильных устройствах программное обеспечение представляет собой код в форме приложения, двоичного файла, модификации фреймворка и т. д. Чтобы предотвратить вред, наносимый таким ПО, и избежать сбоев в работе системы, мы предпринимаем необходимые меры.</p> <p>Правила в отношении нежелательного ПО распространяются и на ПО для мобильных устройств. Мы будем расширять их по мере появления новых видов злоупотреблений.</p> <p>Понятная функциональность и явное раскрытие информации</p> <p>Любой код должен исполнять всё, что обещано пользователю. Приложения должны выполнять все заявленные функции и не должны вводить пользователей в заблуждение.</p> <p>Функции и цели приложения должны быть понятны. Явным образом объясните пользователям, какие изменения в систему будет вносить приложение. Разрешите пользователям просматривать и утверждать все важные параметры при установке. Программное обеспечение не должно искажать информацию о состоянии устройства, например заявлять, что система находится в критическом состоянии или заражена вирусами. Не используйте нелегальные методы для увеличения рекламного трафика и/или конверсии. Запрещены приложения, которые вводят в заблуждение пользователей, выдавая себя за другое лицо (например, другого разработчика, компанию или организацию) или другое приложение, хотя по факту не имеют к ним отношения.</p> <p>Примеры нарушений:</p> <p>мошенничество с рекламой; социальная инженерия.</p> <p>Защита пользовательских данных</p> <p>Явным образом сообщите, как приложения получают доступ к информации пользователя, какие данные собираются и передаются, как они используются. Пользовательская информация должна использоваться в соответствии со всеми действующими правилами. При работе с ней необходимо принимать меры предосторожности.</p> <p>Предоставьте пользователям возможность дать согласие на сбор данных до того, как вы начнете их собирать и куда-либо отправлять (в том числе сведения о сторонних аккаунтах, адресе электронной почты, номере телефона, установленных приложениях, файлах, сведения о местоположении и любые другие личные и конфиденциальные данные, о сборе которых пользователь может не знать). Обрабатывать все личные и конфиденциальные данные пользователя необходимо безопасным образом, в том числе с применением современных методов шифрования, например протокола HTTPS. Программное обеспечение, в том числе для мобильных устройств, должно передавать на сервер только те личные и конфиденциальные данные, которые необходимы для выполнения функций приложения.</p> <p>Примеры нарушений:</p> <p>сбор данных (шпионское ПО); нарушение ограниченных разрешений.</p> <p>Примеры правил в отношении пользовательских данных:</p> <p>Правила Google Play в отношении пользовательских данных Правила в отношении пользовательских данных в рамках требований GMS Правила API Google в отношении пользовательских данных</p> <p>Обеспечение удобства пользователя</p> <p>Взаимодействие с приложением должно быть простым и интуитивно понятным. Приложение должно соответствовать заявленным целям и не вводить пользователя в заблуждение.</p> <p>Если в приложении показывается реклама, она не должна нарушать функциональность устройства и появляться вне среды приложения. У пользователя должна быть возможность дать согласие на ее показ. Кроме того, ее должно быть легко отключить.</p> <p>Приложения не должны влиять на приложения других разработчиков, а также на работу устройства. Процесс удаления приложения должен быть простым и понятным. Мобильные приложения не должны имитировать уведомления операционной системы и других программ. Не отключайте предупреждения других приложений или операционной системы, особенно те, которые информируют пользователя об изменениях в ОС.</p> <p>Примеры нарушений:</p> <p>объявления, прерывающие работу приложения; несанкционированное использование или имитация функций системы.</p>
			Мошенничество с рекламой	<p>Мошеннические действия с рекламными объявлениями строго запрещены. Объявления, которые создают для рекламной сети видимость, будто увеличение посещаемости связано с реальным интересом пользователей – пример мошеннической рекламы и недействительного трафика. К мошенничеству с рекламой могут относиться ситуации, когда разработчики размещают рекламу запрещенными способами, например показывают скрытые объявления, используют автоматическое нажатие на объявления, изменяют информацию или прибегают к иным ручным и автоматическим (роботам, ботам и т. д.) методам генерации недействительного рекламного трафика. Недействительный трафик и мошенничество с объявлениями вредны для рекламодателей, разработчиков и пользователей и в долгосрочной перспективе снижают доверие к экосистеме мобильных объявлений.</p>
			Несанкционированное использование или имитация функций системы	<p>Приложения или объявления, которые содержатся в них, не должны имитировать функции или предупреждения операционной системы и других программ. Системные уведомления можно использовать только для неотъемлемых компонентов приложения. Например, приложение авиакомпании может показывать уведомления о распродажах билетов, а игра – о внутриигровых акциях.</p>
			Социальная инженерия	<p>Запрещено публиковать приложения, выдающие себя за оригинальные, с целью обманом заставить пользователя выполнить действия, которые он совершил бы в исходном приложении.</p>

		Семьи	Разработка приложений, подходящих для всей семьи	<p>Когда родители выбирают контент для своих детей, они хотят, чтобы он был качественным и безопасным. На этой странице рассказано, каким требованиям должны соответствовать приложения, которые предназначены для всей семьи или только для детей.</p> <p>Понятие "дети" может трактоваться по-разному в зависимости от страны и ситуации. Чтобы узнать, какие возрастные ограничения применяются к вашему приложению и какие обязательства вы должны соблюдать как его разработчик, проконсультируйтесь с юристом. Вы знаете свое приложение лучше всех, и только от вас зависит, будет ли оно безопасным для детей.</p> <p>Приложения, разработанные специально для детей, должны быть включены в программу "Приложения для всей семьи". Подать заявку на участие в ней также можно, если в целевую аудиторию входят и дети, и взрослые. Любые приложения, предназначенные для всей семьи, потенциально смогут участвовать в программе "Одобрено преподавателями", но мы не можем гарантировать, что они будут в нее включены. Даже если вы не захотите включать свой контент в программу "Приложения для всей семьи", вам нужно будет соблюдать приведенные ниже требования, а также другие Правила программы для разработчиков и условия Соглашения о распространении программных продуктов.</p>
				<p>Требования к приложению в Play Console</p> <p>Целевая аудитория и контент</p> <p>Перед публикацией приложения необходимо выбрать возрастную группу в разделе Целевая аудитория и контент в Google Play Console. Независимо от того, какую группу вы укажете, мы будем учитывать, есть ли в вашем приложении изображения и фразы, из-за которых приложение можно считать ориентированным на детей. Команда Google Play оставляет за собой право проверять предоставленную информацию о приложении и определять, точно ли выбрана целевая аудитория.</p> <p>Если вы укажете, что приложение предназначено только для взрослых, но Google придет к другому выводу, вы сможете добавить для пользователей ярлык с предупреждением.</p> <p>Несколько возрастных групп можно выбрать только в том случае, если вы точно уверены, что приложение подходит для всех них. Например, контент для малышей и дошкольников должен относиться только к категории "До 5 лет". Если вы разработали приложение для учеников определенного класса, выберите наиболее подходящий возраст. Группы, включающие и взрослых, и детей, можно указывать, только если ваше приложение действительно предназначено для всех возрастов.</p> <p>Обновления раздела "Целевая аудитория и контент"</p> <p>Вы можете в любой момент изменить информацию в разделе "Целевая аудитория и контент" в Google Play Console. Чтобы новые сведения появились в Google Play, необходимо выпустить обновление, однако проверить их мы можем ещё до того, как вы загрузите новую версию приложения.</p> <p>Если вы изменили целевую аудиторию, добавили в приложение рекламу или платный контент, мы настоятельно рекомендуем сообщить об этом пользователям. Для этого можно использовать раздел "Что нового" на странице в Google Play или уведомления в самом приложении.</p> <p>Искажение фактов в Play Console</p> <p>Искажение фактов о приложении в Play Console, в том числе в разделе "Целевая аудитория и контент", может привести к удалению или блокировке приложения, поэтому важно предоставить как можно более точную информацию.</p>
				<p>Требования к приложениям для детей</p> <p>Если дети входят в вашу целевую аудиторию, вы должны выполнять перечисленные ниже требования. Их несоблюдение может привести к удалению или блокировке приложения.</p> <p>Контент приложения. Контент, доступный детям, должен подходить для них.</p> <p>Функционал приложения. Основной целью приложения не должно быть предоставление компонента WebView или привлечение трафика на другие сайты, кому бы они ни принадлежали.</p> <p>Мы постоянно ищем способы дать разработчикам приложений для детей новые возможности. Если вас интересует участие в нашем пилотном проекте Trusted Web App для образовательных приложений, сообщите об этом здесь.</p> <p>Ответы на вопросы в Google Play Console. Вы должны точно отвечать в Google Play Console на все вопросы о своем приложении и обновлять ответы, когда вносите в него изменения.</p> <p>Реклама. Если вы показываете в приложении рекламу для детей или пользователей, чей возраст неизвестен, то должны:</p> <ul style="list-style-type: none">использовать для показа объявлений таким пользователям только рекламные SDK, сертифицированные Google Play;исключить для таких пользователей ремаркетинг (рекламу, направленную на отдельных пользователей и зависящую от истории взаимодействия с сайтом или приложением) и рекламу на основе интересов (рекламу, направленную на отдельных пользователей, чье поведение в Сети соответствует определенным характеристикам);убедиться, что контент в рекламе для таких пользователей можно показывать детям;убедиться, что реклама для таких пользователей соответствует требованиям к формату объявлений для всей семьи;обеспечить соблюдение действующего законодательства и отраслевых стандартов, касающихся рекламы для детей. <p>Сбор данных. Если ваше приложение собирает какую-либо личную или конфиденциальную информацию детей, в том числе с помощью API и SDK, вы должны сообщить об этом в явной форме. К конфиденциальной информации относятся, например, учетные данные, данные с микрофона и камеры, данные об устройстве, идентификатор Android, данные об использовании объявлений и рекламный идентификатор.</p> <p>API и SDK. Убедитесь, что API и SDK используются в вашем приложении надлежащим образом.</p> <p>Приложения, единственной целевой аудиторией которых являются дети, не должны использовать API или SDK, которые не одобрены для рассчитанных на детей сервисов. Это относится в том числе к входу с аккаунтом Google (и другим API Google, которые имеют доступ к данным аккаунта), игровым сервисам Google Play и любым API, которые используют для аутентификации и авторизации технологии OAuth.</p> <p>В приложениях, предназначенных как для детей, так и для взрослых, нельзя использовать API или SDK, которые не одобрены для рассчитанных на детей сервисов. Исключения возможны, если API или SDK применяются только после проверки с помощью нейтрального возрастного фильтра или если при их использовании данные детей не собираются (например, когда вход с аккаунтом Google является дополнительной функцией). Приложения, предназначенные как для детей, так и для взрослых, не должны использовать для входа или получения доступа к контенту API или SDK, которые не одобрены для рассчитанных на детей сервисов.</p> <p>Политика конфиденциальности. На страницу приложения в Google Play необходимо добавить ссылку на свою политику конфиденциальности. Ссылка должна работать все время, пока приложение доступно в Google Play. Политика конфиденциальности, помимо прочего, должна содержать точную информацию о том, как именно ваше приложение собирает и использует данные.</p> <p>Особые ограничения.</p> <p>Если приложение использует дополненную реальность, при ее запуске должно появляться предупреждение, содержащее следующую информацию:</p> <ul style="list-style-type: none">Напоминание о важности родительского контроля.Напоминание об опасности объектов реального мира (например, "Обращайте внимание на предметы и людей вокруг"). <p>Приложение не должно требовать использования устройств, не рекомендованных для детей (например, Daydream или Oculus).</p> <p>Соблюдение законодательства. Ваше приложение, а также все выполняемые или используемые им API и SDK, не должны нарушать Закон США "О защите личных сведений детей в интернете" (COPPA), Генеральный регламент ЕС о защите персональных данных (GDPR), а также другие действующие законы и правила.</p>

				<p>Программа "Приложения для всей семьи"</p> <p>Приложения, разработанные специально для детей, должны быть включены в программу "Приложения для всей семьи". Если ваше приложение предназначено для всех, включая детей и семьи, вы тоже можете подать заявку на участие в этой программе.</p> <p>Перед подачей заявки убедитесь, что приложение соответствует требованиям программы "Приложения для всей семьи" и критериям допуска в нее, а также Правилам программы для разработчиков и условиям Соглашения о распространении программных продуктов.</p> <p>Подробнее о том, как подать заявку на участие в программе...</p> <p>Проверка на соответствие требованиям программы</p> <p>Контент и реклама во всех приложениях, участвующих в программе "Приложения для всей семьи", должны быть рассчитаны на детей и соответствовать приведенным ниже правилам. Эти требования должны соблюдаться все время, пока приложение участвует в программе. Команда Google Play оставляет за собой право отклонять, удалять и блокировать приложения, не соответствующие правилам.</p> <p>Требования программы "Приложения для всей семьи"</p> <p>Приложение должно иметь возрастное ограничение "Для всех" или "10+" (по классификации ESRB) или аналогичное им.</p> <p>При заполнении анкеты для присвоения возрастного ограничения в Google Play Console вы должны сообщить точную информацию обо всех интерактивных элементах приложения, в том числе указать:</p> <ul style="list-style-type: none"> могут ли пользователи взаимодействовать друг с другом или обмениваться информацией; передает ли приложение личные данные пользователей третьим лицам; передает ли приложение информацию о местоположении пользователя другим людям. <p>Приложения, значок которых недопустим для детей.</p> <p>Если ваше приложение использует Android Speech API, значение параметра RecognizerIntent.EXTRA_CALLING_PACKAGE должно соответствовать названию пакета приложения (packageName).</p> <p>В приложениях должны использоваться только рекламные SDK, сертифицированные Google Play.</p> <p>Приложения, созданные специально для детей, не могут запрашивать доступ к данным о местоположении.</p> <p>Для запроса подключения по Bluetooth необходимо использовать класс CompanionDeviceManager. Это правило не распространяется на приложения, предназначенные исключительно для версий ОС, которые не поддерживают этот класс.</p>
			Реклама и монетизация	<p>Реклама в приложениях, участвующих в программе "Приложения для всей семьи" или подпадающих под требования к приложениям для детей, должна соответствовать перечисленным ниже правилам. Они относятся к любой рекламе ваших и сторонних приложений, покупкам в приложении и другому коммерческому контенту (например, к продукт-плейсменту). Ничто из перечисленного также не должно нарушать действующие законы и нормы, в том числе корпоративные и отраслевые.</p> <p>Команда Google Play оставляет за собой право отклонять, удалять и блокировать приложения, слишком настойчиво предлагающих платный контент.</p> <p>Требования к формату объявлений</p> <p>Рекламные объявления и предложения сделать покупку в приложении не должны использовать контент, вводящий в заблуждение, и не должны быть предназначены для того, чтобы провоцировать ребенка на необдуманные нажатия. Запрещены следующие приемы:</p> <ul style="list-style-type: none"> Объявления, прерывающие работу приложения, в том числе занимающие весь экран или мешающие работе с приложением, которые сложно закрыть (например, полноэкранные объявления). Объявления, которые мешают нормальной работе приложения или игры и не закрываются через 5 секунд. Объявления, которые не мешают нормальной работе приложения или игры, могут не закрываться через 5 секунд (например, видеоклип со встроенной рекламой). Межстраничные объявления или предложения совершить покупку, которые появляются сразу после запуска приложения. Размещение нескольких объявлений на странице. Например, одновременный показ более одного баннера или видеообъявления, рекламные баннеры, которые содержат несколько предложений в одном месте размещения. Объявления или предложения совершить покупку, которые сложно отличить от контента приложения. Использование шокового эффекта и тактик эмоционального манипулирования, чтобы провоцировать пользователей на просмотр объявлений или на покупку в приложении. Отсутствие четкого указания на различия между виртуальной валютой и реальными деньгами при покупках в приложении.
				<p>Рекламные SDK</p> <p>При размещении рекламы в приложении, предназначенном только для детей, необходимо использовать рекламные SDK, сертифицированные Google Play. Если приложение рассчитано как на детей, так и на взрослых, вы должны предусмотреть проверку возраста пользователя (например, с помощью нейтрального возрастного фильтра) и убедиться, что дети будут видеть только те объявления, для которых использовались рекламные SDK, сертифицированные Google Play. В приложениях, участвующих в программе "Приложения для всей семьи", запрещается использовать другие рекламные SDK.</p> <p>Подробные требования к объявлениям и ссылке на список сертифицированных рекламных SDK можно найти на странице Программа рекламы в приложениях для всей семьи.</p> <p>Если вы используете AdMob, уточните информацию по работе с ним в Справочном центре.</p> <p>Вы должны самостоятельно проверять, соответствует ли ваше приложение требованиям к рекламе, покупкам в приложении и коммерческому контенту. Уточните действующие правила у своих поставщиков рекламных SDK.</p>
				<p>Покупки в приложении</p> <p>Перед покупкой в приложении, участвующем в программе "Приложения для всей семьи", пользователю нужно пройти повторную аутентификацию. Это гарантирует, что покупку совершает финансово ответственный человек, а не ребенок.</p>
		Другие программы	Приложения для Android с мгновенным запуском	<p>Идентификация</p> <p>Если приложение с мгновенным запуском предполагает вход в аккаунт, в него необходимо интегрировать функцию Smart Lock для паролей.</p>
				<p>Поддержка ссылок</p> <p>Если необходимо перенаправить пользователя из одного приложения в другое, следует реализовать переход в приложение с мгновенным запуском (если это возможно), а не использовать компонент WebView.</p>
				<p>Технические характеристики</p> <p>При разработке приложений с мгновенным запуском обязательно соблюдайте технические требования Google, которые могут меняться время от времени, в том числе требования, перечисленные в открытой документации.</p>

				<p>Предложение установить приложение</p> <p>Приложение с мгновенным запуском может предлагать установить приложение, но это не должно быть его основной функцией. Кроме того, должны соблюдаться следующие требования:</p> <p>Используется стандартный значок Material Design "Установить" и кнопка с надписью "Установить".</p> <p>Используется не более 2-3 скрытых предложений установить приложение.</p> <p>Предложение об установке не похоже на рекламу (например, нельзя использовать баннеры).</p>
				<p>Внесение изменений в устройство</p> <p>Приложение с мгновенным запуском не должно вносить в устройство пользователя изменения, которые сохраняются дольше, чем работает само приложение. Например, оно не должно менять обои или создавать виджет на главном экране.</p>
				<p>Видимость работы приложения</p> <p>Пользователь должен знать, что приложение с мгновенным запуском работает. Скрывать факт работы приложения от пользователя нельзя.</p>
				<p>Идентификаторы устройства</p> <p>У приложения с мгновенным запуском не должно быть доступа к идентификаторам устройства, которые остаются после завершения работы приложения, если при этом пользователь не может сменить их. Несколько примеров:</p> <p>Номер Build Serial; MAC-адреса любых сетевых процессоров; IMEI-код и номер IMSI.</p> <p>Приложение может получить доступ к номеру телефона с разрешения пользователя. Разработчик не должен пытаться определить личность пользователя с помощью этих идентификаторов или других данных.</p>
				<p>Сетевой трафик</p> <p>Сетевой трафик внутри приложения с мгновенным запуском должен шифроваться с помощью протокола стандарта TLS, например HTTPS.</p>
				<p>Эти правила распространяются на любые материалы (включая рекламу и пользовательский контент), которые содержит или показывает ваше приложение либо на которые оно ссылается, а также на общедоступную информацию в вашем аккаунте разработчика Google Play (включая ваше имя и целевую страницу сайта).</p> <p>Запрещено публиковать приложения, которые позволяют устанавливать другие приложения. Если ваши приложения обеспечивают доступ к другим приложениям, играм или ПО без установки, в том числе к функциям, предоставленным третьими лицами, вы должны гарантировать, что весь контент, к которому приложения предоставляют доступ, соответствует правилам Google Play. Такие приложения могут подвергаться дополнительной проверке на соблюдение правил.</p> <p>В правилах используются те же термины, что и в Соглашении о распространении программных продуктов. Ваше приложение обязано соответствовать требованиям правил и соглашения, а также иметь рейтинг в соответствии с нашей системой возрастных ограничений.</p> <p>Запрещено публиковать приложения, подрывающие доверие пользователей к экосистеме Google Play. Принимая решение о публикации приложений в Google Play, мы учитываем ряд факторов, в том числе вероятность вредоносного поведения или злоупотребления. Вероятность злоупотребления оценивается на основе различных сведений, включая историю нарушений, жалобы на приложение и разработчика, отзывы пользователей, а также использование популярных брендов, персонажей и других объектов.</p> <p>Как это работает</p> <p>Google Play Защита проверяет приложения во время установки, а также периодически сканирует ваше устройство. Если будет обнаружено потенциально опасное приложение, сервис:</p> <p>Отправит вам уведомление. Чтобы защитить свое устройство, нажмите на уведомление и выберите "Удалить".</p> <p>Заблокирует приложение, если вы его не удалите.</p> <p>Удалит приложение. Чаще всего опасные приложения удаляются автоматически, после чего появляется уведомление об этом.</p> <p>Защита от вредоносного ПО</p> <p>Чтобы защищать вас от вредоносного стороннего ПО, мошеннических сайтов и других угроз, Google может получать сведения о:</p> <p>сетевых подключениях вашего устройства; потенциально опасных URL; приложениях из Google Play и сторонних источниках, установленных на вашем устройстве, а также об операционной системе.</p> <p>Если приложение или URL покажется нам подозрительным, вы получите предупреждение. Мы оставляем за собой право блокировать и удалять приложения или URL, которые могут нанести вред устройству, данным или пользователю.</p> <p>Вы можете отключить некоторые функции защиты в настройках устройства, но Google по-прежнему будет получать сведения о приложениях, установленных через Google Play. Приложения из сторонних источников все равно будут проверяться, хотя информация о них не будет отправляться в Google.</p> <p>Как работают оповещения о нарушениях конфиденциальности</p> <p>Если мы удалим из Google Play приложение, которое может получить доступ к вашим персональным данным, вы получите уведомление об этом и сможете удалить приложение с устройства.</p>

			Контроль за соблюдением правил	<p>Если ваше приложение нарушает какие-либо наши правила, мы примем меры, описанные ниже. Мы предоставим вам информацию о своих действиях по электронной почте, а также сообщим, как подать апелляцию, если вы считаете, что мы ошиблись.</p> <p>Обратите внимание, что удаление или предупреждение может касаться не всех нарушений, допущенных в вашем приложении или каталоге приложений. Разработчики обязаны сами устранить остальные нарушения и проверить свой контент на соответствие нашим правилам. Если вы не устраните нарушения во всех своих приложениях, мы можем принять дополнительные принудительные меры.</p> <p>Повторные или серьезные нарушения этих правил (например, мошенничество или размещение вредоносного ПО) или нарушение Соглашения о распространении программных продуктов приведет к удалению аккаунтов разработчика.</p> <p>Принудительные меры</p> <p>В этом разделе представлены возможные действия со стороны Google Play и их потенциальные последствия для вашего приложения/аккаунта разработчика Google Play. Также эта информация разбирается в видео.</p> <p>Отклонение</p> <p>Новое приложение или обновление не будет опубликовано в Google Play. Если новая версия приложения отклонена, предыдущая успешно опубликованная вами версия по-прежнему будет доступна в Google Play. Вы сохраните доступ к статистике, оценкам и данным о количестве установок отклоненного приложения. Репутация вашего аккаунта разработчика Google Play не пострадает.</p> <p>Примечание. Не пытайтесь опубликовать отклоненное приложение заново, пока не устраните нарушения.</p> <p>Удаление</p> <p>Приложение, а также все предыдущие его версии, будет удалено из Google Play. Пользователи больше не смогут его скачать. Пользователи не смогут просматривать описание приложения, число установок, статистику и оценки. Информация будет восстановлена, если вы загрузите версию, которая отвечает всем требованиям. Пользователи могут потерять возможность делать покупки в приложении и использовать другие платежные функции, пока новая версия, отвечающая всем требованиям, не будет одобрена Google Play. Удаление не скажется на репутации вашего аккаунта разработчика Google Play. Однако если удалений будет много, действие аккаунта может быть приостановлено.</p> <p>Примечание. Не пытайтесь опубликовать удаленное приложение заново, пока не устраните нарушения.</p> <p>Блокировка</p> <p>Приложение, включая все его предыдущие версии, будет удалено из Google Play. Пользователи больше не смогут его скачать. Серьезные и систематические нарушения правил, а также повторные отклонения и удаления приложения могут привести к его блокировке. Пользователи не смогут просматривать страницу приложения в Google Play, информацию о числе установок, статистику и оценки. Информация будет восстановлена, если вы загрузите версию, которая отвечает всем требованиям. Вы больше не сможете использовать APK и набор App Bundle заблокированного приложения. Пользователи потеряют возможность делать покупки в приложении и использовать другие платежные функции, пока новая версия, отвечающая всем требованиям, не будет одобрена Google Play. Блокировка вредит репутации вашего аккаунта разработчика Google Play. Неоднократные блокировки могут привести к прекращению действия личного аккаунта, а также связанных с ним аккаунтов разработчика Google Play.</p> <p>Примечание. Не пытайтесь повторно опубликовать заблокированное приложение без разрешения Google Play.</p> <p>Ограничение видимости</p> <p>Видимость вашего приложения в Google Play будет ограничена. При этом оно по-прежнему будет доступно по прямой ссылке на страницу приложения в Google Play. Ограничение видимости не повлияет на репутацию вашего аккаунта разработчика Google Play. Пользователи по-прежнему смогут просматривать страницу приложения в Google Play, информацию о числе установок, статистику и оценки.</p> <p>Прекращение действия аккаунта</p> <p>Прекратив действие вашего аккаунта разработчика, мы удалим из Google Play все приложения в вашем каталоге и запретим вам публиковать новые. Все связанные аккаунты разработчика также будут заблокированы навсегда. Повторные блокировки или блокировки, связанные с серьезными нарушениями правил, могут привести к прекращению действия вашего аккаунта Play Console. Поскольку приложения, опубликованные через этот аккаунт, будут удалены, пользователи не смогут просматривать страницы приложений в Google Play, информацию о числе установок, статистику и оценки.</p> <p>Примечание. Если вы попытаете зарегистрировать новый аккаунт, он также будет заблокирован (без возврата регистрационного взноса). Не пытайтесь регистрировать новые аккаунты Play Console, если действие одного из ваших аккаунтов прекращено.</p>
			Сообщение о нарушениях и дальнейшие меры	<p>Подача апелляции</p> <p>Мы восстанавливаем приложения, только если они были удалены по ошибке и не нарушали Правила программы для разработчиков и условия Соглашения о распространении программных продуктов. Если вы внимательно ознакомились с правилами и считаете, что наше решение могло быть ошибочным, обжалуйте его, следуя инструкциям, отправленным вам по электронной почте.</p> <p>Дополнительные ресурсы</p> <p>Если какие-то принудительные меры в отношении вашего приложения или оценки/комментарии пользователей вызывают у вас вопросы, попробуйте найти ответы по ссылкам ниже или свяжитесь с нами через Справочный центр. Обратите внимание, что юридическую помощь мы не оказываем. Если такая помощь вам нужна, обратитесь к юристу.</p>

			<p>Требования к приложению в Play Console</p> <p>Мы стараемся предлагать пользователям Google Play только безопасные и качественные приложения, а разработчикам – все возможности для достижения успеха. Наша задача – максимально упростить процесс публикации.</p> <p>Нарушение правил Play Console может замедлить проверку приложений или даже привести к отказу в публикации. Чтобы помочь вам избежать самых распространенных нарушений, мы составили список рекомендаций ниже.</p> <p>Прежде чем отправлять приложение на проверку, убедитесь, что вы:</p> <ul style="list-style-type: none"> предоставили точные и полные сведения о приложении и его метаданные; указали актуальную контактную информацию; загрузили политику конфиденциальности своего приложения и добавили обязательную информацию в раздел о безопасности и конфиденциальности данных; указали активный тестовый аккаунт, информацию для входа в него, а также другие сведения, необходимые для проверки приложения (например, учетные данные, QR-код и т. д.). <p>Убедитесь, что приложение работает стабильно и корректно, а также представляет ценность для пользователей. Все его элементы, включая рекламные сети, сервисы аналитики и сторонние SDK, должны соответствовать Правилам программы для разработчиков. Если в целевую аудиторию приложения входят дети, убедитесь, что оно соответствует правилам программы "Приложения для всей семьи".</p> <p>Не забывайте, что вы обязаны ознакомиться с Соглашением о распространении программных продуктов и Правилами программы для разработчиков, а также убедиться, что приложение отвечает всем требованиям.</p>	
	Подготовьте свою учетную запись разработчика . Зарегистрируйте учетную запись разработчика и проверьте свои данные учетной записи разработчика верны. Если вы собираетесь продавать товары, настроить свой торговый счет .			
	План локализации . Если вы планируете включать локализованные копии своего приложения при запуске, начните планировать заранее и следуйте Контрольному списку локализации			
	Планируйте одновременные выпуски . Выпуск вашего приложения на нескольких платформах и устройствах максимизирует вашу рекламную деятельность и количество установок, поэтому включите это в свои планы развития заранее. Если вы не можете запустить приложение на всех платформах сразу же запросите контактные данные пользователей и сообщите им, когда ваше приложение будет готово.			
	Проверьте соответствие рекомендациям по качеству . Рекомендации качеству по для всех приложений, а также определенные критерии для приложений для планшетов, телевизоров и автоматических приложений предоставляют шаблоны тестирования. Вы используете их, чтобы подтвердить, что ваши приложения предлагают базовый дизайн пользовательского интерфейса, функции и функции, ожидаемые пользователями Android.			
	Настройте таргетинг на недавний уровень API . Google Play требует, чтобы новые приложения были ориентированы как минимум на Android 9.0 (уровень API 28), а обновления приложений были ориентированы как минимум на Android 9.0, начиная с 1 ноября 2019 года.			

	Создайте свой набор приложений для Android . Когда вы будете готовы сделать свое приложение доступным для пользователей, либо для тестирования, либо в качестве конечного продукта, создайте пакет Android App Bundle в Android Studio. Google Play будет использовать ваш набор приложений для создания, подписания и обслуживания оптимизированных APK-файлов для каждого устройства пользователя, что приведет к уменьшению размера приложения для загрузки и установки.			
	Выполните внутренние тесты . Используйте внутреннюю тестовую дорожку, чтобы довести свое приложение до 100 внутренних тестировщиков, чтобы получить обратную связь, прежде чем сделать ваше приложение доступным для внешних пользователей в закрытой, открытой или производственной версиях. Используйте несколько закрытых тестовых треков для разных версий вашего приложения, прежде чем отправлять их на открытие тестовых треков или продакшн.			
	Спланируйте листинг вашего приложения в Play Маркете . Подготовьте описания, рекламную графику, скриншоты и видеоролики, которые вы добавите на страницу своего приложения в Play Маркете. Убедитесь, что вы добавили ссылку на вашу политику конфиденциальности, если требуется. Локализируйте страницу своего магазина на всех языках, поддерживаемых вашим приложением, и для стран, на которые вы ориентируетесь.			
	Развивайте интерес к своему приложению или игре с помощью предварительной регистрации и настройте настраиваемую страницу со списком предварительной регистрации .			
	Загрузите свой Android App Bundle на закрытую или открытую тестовую версию . Закрытые и открытые этапы тестирования могут значительно помочь в обнаружении проблем с вашим приложением, давая вам возможность исправить эти проблемы и повысить качество вашего первоначального выпуска. Узнайте, как загрузите Android App Bundle и узнайте о лучшие практики для открытых тестов.			
	Определите совместимость вашего приложения с устройством . Сообщите Play Store, для каких версий Android и размеров экрана устройства предназначено ваше приложение.			

	<p>Проверьте отчеты перед запуском . Когда вы загружаете Android App Bundle на закрытую или открытую версию, вы получите предлусковой отчет . С помощью этого отчета вы можете определить проблемы, обнаруженные после автоматического тестирования вашего приложения на широком спектре реальных устройств под управлением различных версий Android.</p>			
	<p>Установите цену вашего приложения и страны распространения . Как только вы определили свой Модель монетизации , настройте свое приложение как бесплатное или платное и выберите страны, в которых оно будет распространяться.</p>			
	<p>Опт- в правильные варианты распространения . Из цен и страницу распространения, подпишитесь на определенные устройства и программы, такие как Wear OS от Google, Android TV и для всей семьи. Google Play может затем просмотрите свое приложение и, после одобрения, сделайте его более доступным для поиска пользователей.</p>			
	<p>Настройте продукты и подписки для продажи в приложении . Подтвердите страны, в которые вы можете продавать, а также валютные и налоговые вопросы, которые следует учитывать. Затем настройте свою учетную запись продавца и добавьте детали и цены для своих продуктов и подписок в приложении.</p>			
	<p>Определите рейтинг контента вашего приложения . Предоставление соответствующей оценки вашему приложению является требованием политик программы для разработчиков, но это также гарантирует, что ваше приложение увидит нужная возрастная аудитория.</p>			
	<p>Окончательная проверка и публикация . Во-первых, вернитесь и дважды проверьте, что вы выполнили все из этого списка. Теперь ты готов к опубликуйте свое приложение в производственном канале. Если вы выпускаете обновление приложения, используйте поэтапное внедрение, чтобы выпускать обновление для все большего числа пользователей. Это позволяет остановить обновление, если вы обнаружите проблему, поэтому вы можете ограничить количество на пользователей это влияет.</p>			
	<p>Продвигайте свое приложение . Начните продвигать свое приложение с Значок Google Play . Ознакомьтесь с нашими другими маркетинговые инструменты и лучшие практики роста, чтобы начать расширять вашу аудиторию.</p>			

	Просматривайте отзывы пользователей и отвечайте на них . Узнайте, что пользователи думают о вашем приложении, и ответьте на их отзывы, чтобы исправить любые проблемы, которые вы, возможно, не заметили при тестировании.			
	Проверьте свои жизненно важные органы . Android Vitals показывает важную информацию на основе вашего приложения, работающего на реальных устройствах, чтобы помочь вам понять и исправить проблемы со стабильностью и производительностью. Улучшение ваших жизненно важных функций приведет к лучшему пользовательскому опыту, большему количеству вовлеченных пользователей и более высоким рейтингам.			